Privacy and Trust in the Ubiquitous Information Society

Analysis of the impact of convergent and pervasive ICT on privacy and data protection and needs and options for development of the legal framework

Deliverable D4: Final study report

27 March 2009

Authored by:
Michael Friedewald and Timo Leimbach
(Fraunhofer ISI)
David Wright
(Trilateral Research & Consulting)
Serge Gutwirth, Paul De Hert and Gloria González Fuster
(Vrije Universiteit Brussel – VUB)
Marc Langheinrich and Iulia Ion
(ETH Zurich)

Edited by:
David Wright
Project Co-ordinator: Michael Friedewald, Fraunhofer Institute for Systems and Innovation Research, Breslauer Straße, 76139 Karlsruhe, Germany, E-Mail: m.friedewald (at) isi.fraunhofer.de


Free University Brussel, Center for Law, Science, Technology and Society Studies, Belgium. Contact: Serge Gutwirth (serge.gutwirth (at) vub.ac.be). http://www.vub.ac.be/LSTS/


Swiss Federal Institute of Technology, Institute for Pervasive Computing, Zurich, Switzerland. Contact: Marc Langheinrich (langheinrich (at) acm.org) http://www.vs.inf.ethz.ch/

The opinions expressed in this study are those of the authors and do not necessarily reflect the views of the European Commission.

Prepared for the European Commission under the contract on “Privacy and Trust in the Ubiquitous Information Society – Analysis of the impact of convergent and pervasive information and communication technologies on privacy and data protection and needs and options for development of the legal framework”.

Contract No. 07/48652-30-CE-0162704/00-33
## Contents

### Executive summary
 ix

### 1 Introduction
 1.1 Context and Objective ................................................. 1
 1.2 Privacy ............................................................................. 2
 1.3 Privacy and data protection from a legal perspective .......... 5
 1.4 Privacy challenges ....................................................... 6
 1.5 Trust ............................................................................... 8
 1.6 Examples of key privacy and trust issues ....................... 10
 1.7 Structure and methodology & criteria of the study ............ 11

### 2 Challenges from technological developments
 2.1 Information collection technologies ............................... 14
 2.1.1 Positioning and tracking technologies ........................ 14
 2.1.2 Identification technologies ....................................... 17
 2.1.3 Activity and ability recognition ................................... 20
 2.2 Communication and dissemination technologies ............ 23
 2.3 New architectures and protocols .................................... 29
 2.4 Information storage and processing ............................... 32

### 3 Challenges from socio-economic developments
 3.1 Privacy-challenging business functions .......................... 38
 3.1.1 Personalised advertising .......................................... 38
 3.1.2 Electronic payment systems ...................................... 49
 3.1.3 Supply chain management ........................................ 50
 3.1.4 Location-based services .......................................... 51
 3.1.5 Digital rights management and intellectual property rights ...... 52
 3.2 Novel businesses and business models .......................... 55
 3.2.1 Cloud computing ..................................................... 56
 3.2.2 Internet Protocol Television (IPTV) and convergence of electronic media .... 57
 3.2.3 E-energy and smart metering ..................................... 58
 3.2.4 E-health ..................................................................... 61
 3.2.5 E-insurance ............................................................. 68
 3.3 Social networks .............................................................. 70
 3.3.1 Facebook, MySpace and other social networks .......... 70
 3.3.2 Blogging ................................................................. 77
 3.3.3 Social tagging ........................................................... 77
 3.4 Second Life – a case study in the convergence of the real and virtual worlds .... 79
 3.4.1 Standards ................................................................. 80
 3.4.2 Privacy breaches ....................................................... 81
 3.4.3 Privacy policy ........................................................... 81
 3.4.4 We want better privacy! ............................................. 82
 3.4.5 The terms of service (ToS) privacy policy .................. 83
 3.4.6 Challenges ............................................................... 84
 3.5 Convergence of companies .......................................... 85
 3.5.1 Google’s acquisitions .............................................. 86
 3.5.2 Microsoft’s acquisitions .......................................... 88
 3.5.3 Yahoo’s acquisitions ............................................... 90
6.3 Other legal challenges

6.3.1 Dealing with the processing of “unprotected” data .......................................................... 153
6.3.2 ISPs and the disclosure of personal data .................................................................. 154
6.3.3 Confidentiality of communications and integrity of information systems .... 156

7 Principal cross-cutting challenges ......................................................................................... 159

7.1 Definitions – personal data, controller and processor ..................................................... 159
7.2 Transparent data collection and use .................................................................................. 161
7.2.1 Who has my data and what are they doing with them? ........................................ 161
7.2.2 Function creep, secondary use .................................................................................. 163
7.2.3 Data concentration ................................................................................................. 164
7.2.4 Raising the awareness of and educating stakeholders .............................................. 165
7.3 Profiling ......................................................................................................................... 166
7.3.1 More personalised services = more data gathering and processing ..................... 166
7.3.2 Search engines ........................................................................................................ 167
7.4 Surveillance .................................................................................................................... 168
7.5 Informed consent ......................................................................................................... 169
7.6 Identity management ..................................................................................................... 171
7.7 Enforcing existing legislation ......................................................................................... 172
7.7.1 Lacunae in existing regulation ............................................................................... 172
7.7.2 Difficulties in enforcing legislation .......................................................................... 173
7.7.3 Data security ............................................................................................................ 174
7.7.4 How to encourage data minimisation ....................................................................... 174
7.7.5 Is there a need to regulate virtual worlds? ............................................................. 175
7.7.6 Regulation vs. self-regulation ................................................................................ 175
7.8 International transfers of personal data and global regulation ..................................... 176
7.9 Trust ............................................................................................................................... 177
7.10 Assessing harm to a person’s privacy .......................................................................... 178
7.11 Balancing values .......................................................................................................... 179

8 Possible responses .............................................................................................................. 181

8.1 Technical responses ...................................................................................................... 182
8.1.1 Privacy-compliant data management ........................................................................ 182
8.1.2 Development tools and libraries for privacy-compliant data handling .................. 182
8.1.3 Supervisory tools for inspection and verification ................................................... 183
8.1.4 Infrastructural support for anonymous communication .......................................... 184
8.1.5 Identity management tools .......................................................................................... 185
8.1.6 Online subject access tools ...................................................................................... 188
8.1.7 Anticipating new technologies and their impacts ...................................................... 188
8.2 Administrative responses and measures ........................................................................... 188
8.2.1 Evaluation of privacy aspects of ICT research proposals .......................................... 189
8.2.2 Standards .................................................................................................................. 189
8.2.3 Open working groups ............................................................................................... 192
8.2.4 Public procurement .................................................................................................. 193
8.2.5 Testing third-country data protection safeguards .................................................. 194
8.2.6 Audits and more resources for DPAs ....................................................................... 194
8.2.7 Benchmarking, metrics and additional research .................................................... 195
8.3 Awareness-raising and education measures .................................................................. 196
8.3.1 Media attention, publicity and public opinion .......................................................... 196
8.3.2 Sharing best practices ............................................................. 197
8.3.3 Public education and awareness raising ........................................ 199
8.3.4 Privacy and trust seals ............................................................... 200
8.4 Self-regulation and other measures .................................................. 203
8.4.1 Codes of conduct ........................................................................ 204
8.4.2 Industry initiatives ................................................................. 205
8.4.3 Training staff ........................................................................ 206
8.4.4 Individual initiatives and consumer actions ................................... 207
8.4.5 Transparency and trust-enhancing responses ............................... 207
8.5 Legal responses ............................................................................ 208
8.5.1 Upgrading personal data protection ............................................ 209
8.5.2 Developing privacy protection .................................................... 212
8.5.3 Embracing the technological dimension ....................................... 215

9 EU level instruments to enact or support the identified measures ........... 217
9.1 Research ....................................................................................... 218
9.2 Demonstration projects ................................................................. 218
9.3 Social dialogue, impact assessments and consultations ....................... 219
9.4 Ensuring an appropriate regulatory framework .................................. 224
9.5 Committees, working groups, platforms and agencies ................. 227
9.6 International co-operation ............................................................ 227
9.7 Procurement .................................................................................. 229

10 Assessments .................................................................................. 231
10.1 Criteria for assessing proposed measures ....................................... 231
10.2 Indicators for assessing implementation of policy options ............... 233
10.3 Assessment of response measures .................................................. 235
10.3.1 Transparency tools .................................................................... 235
10.3.2 Data control tools ...................................................................... 237
10.3.3 Privacy impact assessments ......................................................... 240
10.3.4 Evaluation of privacy aspects of ICT research proposals ............... 243
10.3.5 Public procurement ................................................................... 245
10.3.6 Standards .................................................................................. 247
10.3.7 Audits and metrics ..................................................................... 249
10.3.8 Media attention, publicity and public opinion .............................. 252
10.3.9 Sharing best practices ................................................................. 254
10.3.10 Public education and awareness-raising ..................................... 256
10.3.11 Privacy and trust seals ............................................................... 259
10.3.12 Regulatory suasion .................................................................... 261
10.3.13 Codes of conduct, guidelines and other privacy exhortations .......... 264
10.3.14 Legal responses ........................................................................ 267
10.3.15 Anticipating new technologies and their impacts ....................... 269

10.4 Assessment of responses to challenges .......................................... 271
10.4.1 Legal definitions ........................................................................ 271
10.4.2 Data collection and use .............................................................. 272
10.4.3 Raising the awareness of and educating stakeholders .................. 274
10.4.4 Profiling ................................................................................... 278
10.4.5 Identity management ................................................................. 279
10.4.6 Surveillance ............................................................................... 281
10.4.7 Informed consent ...................................................................... 283
10.4.8 Enforcing existing legislation ...................................................... 284
10.4.9 International transfers of personal data .......................................................... 286
10.4.10 Trust ............................................................................................................... 291
10.4.11 Harms to individual privacy ........................................................................... 293
10.4.12 Competing values and interests ...................................................................... 296

11 Conclusions and recommendations ............................................................................ 301
11.1 Findings of fact ........................................................................................................ 301
11.2 Recommendations .................................................................................................... 303
EXECUTIVE SUMMARY

It is perhaps stating the obvious to say that new and emerging technologies, especially those that are leading us towards the ubiquitous Information Society, present fundamental challenges to notions of privacy and trust, however these are defined and whoever might hold such notions. These developments require policy-makers, industry and other stakeholders to assess existing policies and safeguards and, if necessary, build in new ones that will better protect the privacy and preserve the trust of citizens. This is not to say that curbs or restrictions need to be placed on the technologies or their further development. Society's attention should rather be on how those technologies are used, to which needs and prospects they respond, who uses them and for what purpose.

This study is to provide information helping to develop and assess policy options at EU level addressing existing and new challenges to effective data protection, privacy and trust resulting from the emergence of the ubiquitous Information Society. Moreover, it aims to provide input for the development of a set of EU level measures responding to the challenges, based on an assessment of available instruments to achieve the maximum potential benefits. It identifies various specific challenges to privacy and trust in the ubiquitous Information Society that are resulting from technological developments and from new privacy-infringing business-models and administrative practice. It explores how well the existing legal framework is prepared for the future.

Consequently, the report is organised in two main parts: The first deals with the identification and analysis of challenges and the second with possible policy responses.

The general approach followed in preparing the first part has been to identify challenges to privacy and trust from technological developments (Chapter 2), socio-economic developments (Chapter 3), administrative developments (Chapter 4) and the special case of international transfers of personal data (Chapter 5). Chapter 6 addresses legal challenges, while Chapter 7 summarises the main, cross-cutting challenges, i.e., those that recur across different developments. The identification of privacy and trust issues (challenges) raised by the ubiquitous Information Society was based on a rather exhaustive sweep and compilation of documents dealing with privacy and trust issues.

The second part of the study deals with possible responses to privacy and trust challenges. Chapter 8 collates and summarises possible responses, while Chapter 9 outlines which instruments are at the disposition of the Commission. In Chapter 10, we define criteria for assessing response measures and use them to assess the response measures and responses to the challenges as summarised in Chapter 7. Finally, we draw our conclusions from this study in Chapter 11.

Challenges from technological development

Chapter 2 of the study explores how new information and communication technologies may shape and challenge the notion of privacy, which has never been stable and has always been subject to a negotiation process between social groups before the background of technological progress.

Warren and Brandeis' seminal definition of “privacy” was triggered by the insight that new technology (photography in 1890) was a “game changer” – a technological shift that
challenged the established notions of privacy and trust in society. Obviously, it was not simply the shrinking of photographic equipment into portable devices, combined with shorter exposure times, that changed these notions. It was the use of the technology in the context of an application – the yellow press and their first photo reporters, who used those portable cameras to take pictures without the consent of the subject. Consequently, any technology-centric view is by definition incomplete – it is typically the application of technology that determines whether it is beneficial or detrimental to our physical and psychological well-being. However, as Melvin Kranzberg notes in his First Law of Technology, “Technology is neither good nor bad. Nor is it neutral.”

Looking at current technological trends, we can group developments roughly according to their (technological) function within the data processing cycle: from information collection technologies to communication technology, and from information exchange technologies to storage and processing. At the outset, we are witnessing an ever improving ability of automated identification, pertaining to things, people and actions. Simple identification technologies such as RFID are nothing more than electronically readable numberplates, yet their widespread use in logistics and retail might have the effect of allowing the implicit identification of people and their affairs (i.e., hobbies, health, interests). RFID, as well as other identification technologies such biometrics or near-field communication (NFC), not only identify things, they also locate them in time and space: Whenever an item or person is identified, the location of this identification can be used to track the movements of things and people over time. This naturally leads to location technology such as GPS or ultra-wide band (UWB), which allow for more fine-grained and continuous positioning. Basic communication technologies such as Wi-Fi, Bluetooth and GSM/UMTS can also be used to locate people and things, which significantly lowers the cost of deployment and use. Beyond knowing who you are and where you are, recent developments have also successfully determined what you do. These activity recognition technologies use data mining and image recognition to automatically detect and classify behaviour. Applications range from SmartCCTV surveillance (in order to detect, e.g., car thieves in a parking lot) to search query analysis and brain wave monitoring. Obviously, activity recognition has also the potential to predict future actions, especially in the context of brain wave scanning or DNA fingerprinting.

Communication technology does not provide data collection options per se, but it significantly lowers the cost to disseminate and process personal information. It thus enables an unprecedented digitalisation of everyday activity (which in turn then allows inference of activity, social relationships, location, etc). Two recent developments are notable and have a great impact: (1) the comprehensive availability of wireless communication technology across any distance, far and near, and (2) the decreased data transmission cost. Of special interest are wireless communication technologies such as Wi-Fi, WiMax, UMTS and Wireless USB, as they offer data collection anywhere, anytime. So-called “reality mining” research uses cell phones to comprehensively monitor, in real-time, the actions of hundreds of participants: who do they call, who do they meet, where are they going? On a much smaller scale, body area networks enable wireless communication along the human body, e.g., for health applications, where multiple small sensors embedded in clothing can conveniently be queried and controlled with minimal energy. Communication technologies also strongly influence information dissemination, i.e., the spreading of collected information. Instant blogging (“to twitter”) and lifelogging are two trends made possible by the proliferation of “always-connected” technologies.
This multitude of information streams needs to be bundled and analysed, in order to make sense of it. Novel information architectures and protocols, such as database federations, the Internet of Things, and Web 2.0, specifically target the integration of a large set of heterogeneous information sources. New technologies for (personal and industrial) information and application sharing pose challenges to privacy and trust, including specific threats from secondary data collection, content-based image retrieval, phishing, infiltration and widespread distribution of user-created content. This also includes the issue of linkability from image metadata, online reputation, online gossip, etc. Some technologies, such as digital identity standards, can be regarded as a possible response to increased data collection, by offering credential-based authorisation options. Note that this trend to open platforms and interoperability, as witnessed in the Web 2.0, is also spreading to the mobile phone market, as witnessed by the Google Android platform in November 2007 and the release of the Apple iPhone software development kit (SDK) in March 2008.

Last but not least, falling prices for digital storage media have led to a significant increase in data storage: Instead of having to minimise data collection due to the associated cost of storing it, today it is much cheaper to simply buy additional storage instead of having to perform a costly analysis of what to store. The availability of cheap storage has already turned into a business model: Cloud computing services such as Amazon’s S3 offer redundant online storage for a few cents per gigabyte per month, attracting not only individuals who store their holiday pictures on Amazon’s servers, but also companies and even health care providers (e.g., Google Health). Offline storage space is equally expanding rapidly, with terabytes of storage retailing for less than 200 Euros (as of August 2008). This proliferation of storage not only affects data collection practices of public and private bodies, but also increases the risk to individuals who collect data that might cause embarrassment (to themselves if not to others), makes them vulnerable to criminal acts such as data or identity theft and could provide incriminating evidence against themselves in the context of criminal or civil investigations. With the availability of ever smaller storage devices that allow people to carry with them vast amounts of data, a considerable volume of which could be personal, there is also an increasing risk of loss or theft.

**Challenges from socio-economic developments**

Chapter 3 identifies and describes a range of socio-economic developments that challenge privacy. The chapter is divided into seven main sections. The first addresses privacy-challenging business functions, including personalised advertising, which is sometimes referred to as behavioural targeting or behavioural advertising. Although different terminologies are in use, it essentially describes the practice whereby a user can be targeted with adverts based on what is known about him or her, the websites they visit, the search terms they use. Also covered here are electronic payment systems, supply chain management, location-based services and digital rights management (DRM).

The second section covers the challenges to privacy and trust arising from novel businesses and business models, including cloud computing, IPTV, e-energy, e-health and e-insurance. While these new business models offer substantial benefits, including significant cost-savings, they often come at the expense of privacy. For example, with cloud computing, users can use (often free) online software and store all of their files in the “cloud” with nominally easy access whenever they want. However, the more data they process and store online, the greater is the risk that third parties will use it in ways not originally foreseen by the user or the storage service. With e-health, we can see a huge increase in the number of people who might
have access to our health records and, again, repurpose the data in ways not originally specified.

The third section deals with social networks, such as Facebook and MySpace, blogging and social tagging. The huge popularity of social networks has many implications for privacy, especially when third-party developers are able to exploit personal data. While there is no denying their popularity and success, they have also been subject to criticism.

In the fourth section, we look at the virtual world of Second Life as a case study in the convergence of the real and virtual worlds and what that means for privacy. A key issue there is whether a person’s avatar should have privacy rights and whether online worlds should be subject to some real-world regulation.

In the fifth section, we examine the increasing concentration of, especially, search engines and advertising companies, perhaps best typified by Google’s acquisition of DoubleClick. Regulators so far have been examining the significant mergers and acquisitions in terms of their impacts on competition, whereas the privacy impacts have received virtually no regulatory scrutiny.

Cybercrime continues to be a social, economic and individual problem, often highly intrusive of individual privacy. It’s not a new phenomenon, and not likely to go away anytime soon. Indeed, indicators suggest the problem is getting worse, not just in scale but also in sophistication of the malware.

The final section examines the relationship between privacy and trust, the factors that shape it, trust models and trust strategies. It considers the success of Amazon which holds a lot of personal information about its customers and which even makes it obvious that it does (for example, by recommending particular books based on our previous purchases and page views), yet Amazon enjoys a high level of trust and good will on the part of its customers.

**Challenges from administrative developments**

Chapter 4 deals with privacy challenges that result from different government activities. It covers several areas within the field of e-government.

A general introduction outlines the broad field of e-government activities. Different activities are defined and described to get a better understanding for the needed research. This is followed by an analysis of some problems posed by e-government applications from the point of EU. Further on, it cites challenges for the implementation of e-government applications. The result of these analyses are illustrated and explained in two major examples.

The first case describes various developments around identification documents, mainly electronically enhanced passports and the European attempts to define a unified electronic identification scheme. The analyses of the state of art on biometric documents as well as electronic identities shows most clearly the problems discussed in general in the chapter's introductory remarks. The status of identification documents and electronic identities several EU Member States and a few other non-EU countries is described.

Our second case is about smart transportation systems. It distinguishes systems aiming to control and regulate the individual use of streets and public transportation systems operated
by private or government enterprises. In individual traffic, data is mainly collected for traffic guidance - either in the form of telematic traffic guidance systems or indirectly through tolls and other pay-as-you-drive schemes. In public transportation, personal data is mainly collected via the various payment schemes using RFID-enabled tickets or mobile devices. Any of these applications give the opportunity to derive mobility profiles for large segments of the populations. Especially when operated by private firms, there is the risk (or even the explicit intention) to use the collected data for secondary purposes, such as marketing. If the data are collected by government authorities, many people assume it is used for surveillance and law enforcement activities.

A final section touches upon the problems around electronic democracy. Since e-democracy has the goal to create an environment that enables people to exercise their civil rights, privacy, anonymity and trust are crucial to the success of e-democracy schemes.

**International transfers of personal data**

Chapter 5 deals with the problem of international transfers of personal data. Many privacy-threatening activities may occur beyond the reach of European regulatory power. We analyse how personal data are transferred abroad and what measures have been adopted and contemplated for protecting our personal data.

**Legal challenges**

The assessment of the current EC legal framework for privacy and data protection in light of the expected developments of the ubiquitous information society reveals various limitations and inadequacies. At the centre of the legal framework stands Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (the e-Privacy Directive), to be read in conjunction with Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the Data Protection Directive).

Some key notions and principles of data protection law appear to be dramatically challenged in the new environment. While actors struggle to agree on a consensual interpretation of the definition of “personal data”, data collecting and processing increase exceptionally, and it becomes clearer that many categories of data, which are not “personal” data per se, can have a direct impact on individuals. The boundaries between the notion of “data controller” and “data processor” become blurred. Determining which national law is applicable in certain cases can be extremely difficult and does not always result in convincing conclusions. It is unclear how “consent” to the processing of data should be obtained, given, proved and withdrawn in certain circumstances. Information provided to the public on processing activities, and especially on profiling practices, is generally unsatisfactory. European case law and some national developments trigger the question of whether it should be necessary to further clarify at EC level when electronic communication service providers should disclose identities of subscribers, and when they should refuse to do so. In general, the limits of the scope of application of Directive 2002/58/EC tend to become difficult to ascertain, and sometimes difficult to justify. The limited protection of the confidentiality of communications and the vulnerability of stored communications, coupled with their continuously increasing importance for individuals, call for innovative solutions.
The legal responses to address the different (both legal and non-legal) identified challenges pertain to three distinct categories. A first category concerns the upgrading and enhancement of personal data protection law. Under this approach falls the need to further work on the clarification of key data protection concepts, the establishment of more concrete requirements in relation with consent, detailing the conditions for the lawfulness of processing, simplifying the determination of applicable law, clarifying obligations for the disclosure of personal data, empowering data protection authorities and effectively encouraging enforcement. A second category of responses aims at effectively developing the right to privacy, notably by ensuring the privacy of communications, possibly through the protection of the integrity and confidentiality of information systems, and by developing the right of the individual to be left alone, in particular through a regulation of “unsolicited adjustments”. A third category of responses focuses on the protection of privacy by reacting to specific technological developments, and refers to the need to reinforce the regulation of specific categories of data, such as traffic and location data, and by launching the legal recognition of other categories of data deserving special protection, such as “unique identifiers”.

These three approaches can be envisioned as layers of protection complementing each other. They take into account the different nature of the right to privacy and the right to data protection, emphasising the need to provide effective protection for both European fundamental rights, and underlining that any attempt to limit the legal protection of privacy to a regulation of the processing of “personal data” is condemned to fail in the ubiquitous Information Society. Taking into account the principles of subsidiarity and proportionality, European legislators must determine how to best actualise them.

Principal cross-cutting challenges

The analyses in Chapters 2 to 6 shows that many challenges are not specific to technology, business or government applications or the legal framework. Chapter 7 summarises cross-cutting challenges:

Legal definitions – personal data, controller and processor: Some have questioned the definition of personal data in the Data Protection and e-Privacy Directives. Clarification of the concept appears to be a required response in the light of its persistent divergent interpretations, especially in the context of new practices, leaving grey areas. The basic requirements for such elucidation should be that the definition is operative and that it effectively protects individuals. It has also been pointed out that any re-definition of the notion should consider the possible need to refocus protection away from the “personal” dimension of the data. However, clarification of the concept of personal data could also be left to eventual judicial review.

Data collection and use: Another important issue, which has been raised many times, is this: Is the control over personal data a special form of personal rights? Or do people own their own personal data as a tradable good? Who then “owns” the personal data supplied by a customer who wants to get a mortgage, life insurance, a discount on his grocery bill, an extended warranty on a product or a new Internet service? Once people have provided their data to a service provider (for example), do they still own the data? Or does the data now belong to the service provider to do with them what he will? Or is the “ownership” shared? That is, the controller can use the data only for specified purposes and must provide access to the data to the individual so that the data can be corrected if necessary? How can we be assured that the service provider will adequately protect our data?
Inadequate privacy awareness and careless handling of personal data: The Commission, data protection authorities and other stakeholders face a challenge in raising the awareness of and educating stakeholders about challenges to privacy and trust. If use of e-government and e-commerce services is to become more widespread than they are now, the Commission, DPAs and other large stakeholders need to increase their investment in awareness-raising and education. Similarly, if we are to curtail the losses caused by cyber criminals and other malefactors, for example, through identify theft and malware, illicit surveillance and electronic espionage, the public must be better educated.

Profiling: In general, it is assumed that most consumers like personalised services. But the more services are personalised, the more personal data are needed by the service provider. It is not just industry that is engaged in data mining and fusing data. Governments are profiling citizens as well, mainly for containing terrorism and law enforcement. Should there be legal requirements governing fusion of personal data? One can envisage the fusion of multiple position reports from different devices in order to derive detailed movement profiles. Though location-based services are not yet very widespread, powerful technologies can build mobility profiles even today using the signals of mobile telephones. We mention other examples of how new technologies lead to more personalisation and profiling, including Internet Television (IPTV) and smart metering of energy consumption.

Search engines, which have been described as “a gateway to the Information Society”, target advertising at the user based on the search terms he or she uses. They log the user’s IP address and over time collect lots of data on the user’s interests. Many of the search engine operators, particularly Google, allow users to store photos, videos, e-mail messages, calendars, all kinds of documents, bookmarks etc. No category of information seems to be too personal, as the Google Health service shows. The accumulation of vast amounts of personal data raises numerous challenges to privacy and trust for Europeans. One key issue is the extent to which European users are protected by European law from the use of personal data by Google and other search engines, the repurposing and security of those data.

Identity management can be seen both as a response and as a challenge. This depends strongly on the technical approach chosen to model an identity layer in the current Internet. Current identity management consists of dozens and hundreds of separate accounts created at every website where the user wants to be known. Even though these accounts are held at separate entities and use freely chosen usernames (pseudonyms), they are often joined together by one and the same contact e-mail address. Furthermore, it is hard to keep track of the number of accounts created, as well as the information held (and its validity) in each of them.

New surveillance: Citizens are surveilled in many different ways, by video cameras, microphones, on the Internet. Their communications may also be monitored. The reality is that surveillance is increasing, feeding into vast databases run by law enforcement authorities and intelligence agencies. Apart from issues such as the security of such vast databases or the misuse and abuse of such data, the more fundamental question is: Is a surveillance society the kind of society we want? While many commentators are still referring to an Orwellian vision, the reality of surveillance is different. While in Orwell’s novel 1984, it was clear that “Big Brother is watching you”, the “new” surveillance systems are less visible and more continuous in time and space, provide fewer opportunities for targets to object to or prevent the surveillance, are greater in analytical power, are disseminated faster and more widely, and are less expensive than the “old” surveillance techniques.
Ill-informed consent: The obligation to inform individuals about the processing of their data is one of the fundamental principles of the Data Protection Directive. However, there is wide consensus supporting the notion that it might be too easy to get apparently “informed” consent. If we want particular products or services, we may need to give our consent to service providers or product suppliers to do what they will with our data, at the expense of our privacy and perhaps even our dignity. Many consumers, especially young people, appear as if they did not attribute much value to their privacy just because they seem willingly to give so much away on social networking websites and in many other ways, with apparently little or nothing in exchange.

Inadequate enforcement of existing legislation: A crucial question is how well existing legislation is being applied, how existing legislation can be better enforced, whether incentives can be devised to encourage companies to comply with data protection principles, whether existing legislation is up to the task of dealing with new technologies, applications and services that were not foreseen when the legislation was introduced. One problem with the e-Privacy Directive is the limited scope of application of most of its provisions. It is limited to the supply of public electronic communication services in public networks and does not take into account the increasing importance of private communication networks, nor the need to protect individuals from being monitored in such circumstances. Nor does it take into account the progressive blurring of public and private communications networks. Also, applications such as social networking sites tend to blur the distinctions between service providers and users/consumers. It remains to be determined whether the concept of controller as exists in the current European legal framework for data protection is still relevant and operational when end users are progressively becoming the main actors in the processing of personal data.

International transfers of personal data: The complexities of international transfers of personal data remain a potent and not adequately resolved issue. Concerns have often been expressed about the difficulty of enforcing EU law once personal data have been transferred from the EU to third countries.

The trust deficit: The consumer-citizen’s trust in government and industry has taken a serious hit recent times as the press propagate stories about personal data that have gone missing, been hacked or otherwise abused. It seems almost daily there are new reports of data losses. In addition, the Internet has its fair share of cyber criminals and cyber bullies as well as data miners, data aggregators and corporate warlords seeking to harvest and exploit as much personal data as possible in order to sell us something. Creating or rebuilding trust is a serious challenge in this environment, yet necessary if beneficial e-government and e-commerce services are to flourish.

Harms to individual privacy: Strictly speaking, assessing harms to a person’s privacy may not be a challenge to privacy as such but rather an open research question. Nevertheless, to respond to the challenges of privacy and trust in the ubiquitous Information Society, it seems highly desirable to understand, measure and deal with the harms caused by intrusions upon the individual’s privacy as well as theft of his or her identity.

Competing values and interests: Stakeholders are continuously balancing privacy against other values. The challenge is to define and reinvent privacy in a continuously changing environment without abandoning crucial values. Policy-makers and regulators are pulled in
different directions, between the needs to balance personal data protection and encouraging economic growth, between privacy and surveillance.

**Possible responses**

In Chapter 8, we identify a range of responses to the challenges. These are technical responses, which include privacy-compliant data management, development tools for privacy-compliant data handling, supervisory tools for inspection and verification, infrastructural support for anonymous communication, identity management tools and online subject access tools\(^1\). At the core of any comprehensive solution must be an information storage concept that is able to process data *in compliance* with the collection policies under which the information was obtained. Such an infrastructure forms the basis for providing any higher-order services such as compliance verification and auditing, online subject access, or anonymisation. While providing the user with easy-to-use tools for online subject access is a good idea, the right to data correction and deletion might conflict with audit requirements.

The technical section concludes with some thoughts on anticipating new technologies and their impacts. *Privacy and usage of privacy-enhancing technologies in collaboration platforms and within Web 2.0 communities are research fields that need further investigation.*

The second class of responses, administrative measures, are essential to respond to the challenges posed by the deployment of ubiquitous computing technologies, because they can reach all phases from R&D to deployment. Administrative measures and responses should aim for an integration or fair balance of the interests of all stakeholders. The possible domains of such measures and responses can be separated in three layers: first, direct responses and actions of public administrations; second, public authorities can initiate measures to create public awareness; and, third, enforcement and regulation of co-operation between producers and consumers. Within all three levels, governments, industry associations, consumer rights groups and other civil society organisations can play an important role to the benefit of all affected groups.

Administrative measures include measures such as evaluating the privacy aspects of ICT research proposals (e.g., proposals made to the Commission under its Framework Programmes), standards, open working groups, procurement measures, testing third-country data protection safeguards (e.g., are non-European countries upholding their commitments to safeguard data transferred from the EU?), audits and more resources for data protection authorities, and metrics. Just how useful various measures are in responding to privacy and data protection challenges will usually require some benchmarks. We need some way of measuring how successful privacy protection is or has been, some metrics that would address, for example, the following:

- How many enforcement actions have been taken by data protection authorities?
- How many successful prosecutions have there been?
- How much have offenders been fined or otherwise penalised?
- From what sectors have offenders come?
- What initiatives have data protection authorities taken to inform the public (data subjects) and data controllers about the arcana of data protection law?

---

\(^1\) See section 8.1.6 for more on this. Essentially, online subject access tools would enable an individual (the data subject) to access her personal information online, to see what a data controller was holding.
• Is citizen awareness of privacy issues and how personal data can be protected improving?

This last point brings us to a third class of responses involving awareness-raising activities and here we include not only stories in the press that highlight threats to privacy, but also measures such as sharing best practices, public education and the use of privacy and trust seals.

Self-regulation forms another class of responses wherein we group measures such as regulatory suasion, codes of conduct, industry initiatives, training staff, individual initiatives, and transparency and trust-enhancing responses. While governments can play an active role in adopting legislation, promulgating guidelines or initiating education programmes, their role in self-regulation can be characterised as supportive of measures (nominally) initiated by industry to avoid the heavier hand of regulation. The advantages of such measures are that they can supplement governmental measures such as research guidelines and codes of conduct and that they can be agreed and put in place more quickly than measures that need to go through several bureaucratic hoops. Governments and regulators often prefer self-regulation to legislation that may be difficult to enforce. However, self-regulation can be problematic in creating unbalanced, asymmetric solutions which may not adequately address the perceived problem or which may delay or sideline more appropriate solutions such as standardisation.

Finally, we set out some legal responses. Legal responses supporting privacy and trust must also contribute to other aims such as the development of new technologies, the promotion of competition, the protection of consumers and the protection of the general interest. The legislative process preceding the adoption of any EC legal instruments is crucial to ensure that all aspects of the responses envisaged are duly taken into account in their eventual deployment. The legislative process allows for the integration of different stakeholders’ concerns, as well as the eventual redefinition of the response for better implementation.

Generally, we are of the view that responses should be incentive-driven, i.e., that stakeholders have incentives to “do the right thing” in addressing the challenges. For example, an EC trust seal might be seen as something service providers will want to have on their home pages because it gives them credibility with consumers, but to be granted a trust seal, they need to take certain privacy-protecting measures. Similarly, if the EC funds development of privacy-enhancing technologies through its Framework Programme, industry is likely to want to invest some time and effort in responding to calls for proposals and making sure that any technologies developed are marketable.

Legislation and regulation are usually only effective to the extent that they can be enforced. It may not be possible to catch everyone guilty of abusing the market, but at least enough have to be caught and penalised so that one can assume, rightly or wrongly, that the legislation or regulation is working and that it is having a deterrent effect. Otherwise, the unenforceability of legislation risks further undermining public trust and confidence. In this regard, determining which responses (e.g., regulation vs self-regulation) are viable is a tricky business.

The European Commission has a set of instruments at its disposal which it can use to support and trigger the implementation of responses, and these are discussed in Chapter 9. Among these instruments are research, demonstration projects, social dialogue, impact assessments (and especially privacy impact assessments) and consultations, expert committees, international co-operation and procurement. As an instrument, social dialogue initiated by the
EC can take different forms. The EC can issue press releases, can encourage citizens to use its websites such as “Your Voice in Europe”, convene workshops and conferences or speak at those organised by others, can have Commissioners and their staff speak on the various issues of the day. Eurobarometer can survey European opinion. The Commission can initiate public consultations. Consultations have many benefits, for example, in identifying pros and cons, in gathering information that policy-makers might not have considered adequately, in moving toward consensus among stakeholders, in testing policy options, as a public relations exercise (in the best sense of that term) in giving stakeholders, including the public, an opportunity to air their views, as an exercise in democracy, and so on.

We give some examples of which instruments can be used to implement which responses. In some cases, a response can be implemented by means of more than one instrument. We also distinguish between impact assessments and privacy impact assessments.

Assessment of policy responses to address privacy challenges

Chapter 10 is in four parts, the first of which sets out some criteria for assessing proposed measures. Building on the Commission’s own impact assessment criteria the responses have been assessed on the basis of following criteria: (1) effectiveness; (2) stakeholder support; (3) time; (4) opacity; (5) transparency; (6) enforcement; (7) economic effects; (8) social impacts (other than privacy protection); (9) compliance of policy options with existing EU initiatives and (10) effects of measures on national legislation.

The second section deals with indicators for assessing implementation of policy options. In other words, the first set of criteria can be regarded as applicable ex-ante, while the second are ex-post.

In the third section, we apply the criteria discussed in the first section to assess the response measures identified in Chapter 8, which are among the most important for dealing with challenges to privacy and trust.

In the fourth section, we present an analysis of the advantages and disadvantages of each of the responses which we find appropriate to the challenges summarised in Chapter 7. This is a core section of the report.

Conclusions and recommendations

The last chapter of the report contains our conclusions and recommendations. The chapter includes some “findings of fact” as well as our recommendations. Our analysis shows that one cannot hope for any silver bullets that will solve the challenges to privacy and trust. Responding to the challenges to privacy and trust posed by the ubiquitous Information Society will require a mix of measures, and most of these measures are already being used today in one form or another, to a lesser or greater extent. The issue is not really finding some new instrument that will cure all problems over night, rather the issue is identifying the challenges as they emerge, which requires good horizon-scanning, and then deciding in consultation with stakeholders on the appropriate measures, taking into account the criteria which we have identified in Chapter 10 of this study.

The following is a summary of our recommendations to the Commission:
1. Develop a common framework for privacy impact assessments and make them
mandatory.

2. Require audits of international transfers of personal data.
3. Companies and government departments should include in their annual reports a description of their data protection measures and an assessment of privacy risks and responses. They should implement the relevant measures (e.g., audits, training staff).
4. Improve legal responses.
5. Data protection authorities should have the authority to conduct audits of public and private sector privacy practices.
6. Develop and use online subject access tools.
7. Identify, analyse and promote good practices.
8. Develop a methodology to measure and assess privacy risks and user trust.
9. Report and publish data breaches, data losses and other privacy infringing incidents.
10. Anticipate new technologies and their privacy impacts.
11. Regulators should review transfers of personal data.
1 INTRODUCTION

1.1 CONTEXT AND OBJECTIVE

It is perhaps stating the obvious to say that new and emerging technologies, especially those that are leading us towards the ubiquitous Information Society, present fundamental challenges to notions of privacy and trust, however these are defined and whoever might hold such notions. These developments require policy-makers, industry and other stakeholders to assess existing policies and safeguards and, if necessary, build in new ones that will better protect the privacy and preserve the trust of citizens. This is not to say that curbs or restrictions need to be placed on the technologies or their further development. Society's attention should rather be on how those technologies are used, to which needs and prospects they respond, who uses them and for what purpose.

More than a century ago, Warren and Brandeis defined privacy as the right to be let alone and their concern about privacy was prompted by a new technology, i.e., photography. Their perceptions then have some interesting parallels with today when some have expressed concern about our already living in a surveillance society. Surveillance cameras are proliferating in our cities, highways and elsewhere. While facial recognition technologies have not yet developed to the point where it is routinely possible to identify anyone who is captured on a video, we can suppose that day will come, and perhaps sooner than some might think. But concerns about living in a surveillance society often melt away in the face of a terrorist attack or a terrorist attempt, when the public is relieved that there are surveillance cameras and that they help to identify would-be terrorists quickly.

Similarly, there are concerns about millions of citizens populating national DNA databases, but those databases have been instrumental in apprehending many rapists, murderers and other evil-doers, sometimes many years after a crime has been committed. Others may express concerns about a national network of digital medical records, its potential for abuse, but if it can save lives, lead to faster and more accurate treatment, then how should policy-makers and health authorities respond?

Many citizens voluntarily provide personal information to commercial social networking websites such as Facebook and MySpace, often disclosing private details without realising or caring that this information not only may be disclosed to a potentially very large audience, but also that it will be indexed and thus become trivially locatable. Similarly, some people are prepared to give away personal data in exchange for the perceived benefits of a supermarket loyalty card, even though they object to being sent unwanted advertising.

Beyond the voluntary exchange of personal data, people are often compelled to surrender their personal data in order to gain something. To get a mortgage, borrowers must provide the lender with personal data. It can be argued, of course, that borrowers have a choice here – they can choose not to give up such data, but the downside is that they do not get the mortgage.

Thus there are lots of ambiguities, uncertainties and risks today concerning our privacy and trust, but in a ubiquitous Information Society, these ambiguities, uncertainties and risks will

---

multiply many times over. When virtually every manufactured product is embedded with an
electronic tag, when “things” can communicate, the complexity and difficulty in developing
privacy-protecting and trust-enhancing policies will escalate further.

This study addresses existing and new challenges to effective data protection, privacy and
trust resulting from the emergence of the ubiquitous Information Society and identifies
possible responses. It identifies various specific challenges to privacy and trust in the
ubiquitous Information Society resulting from technological developments and from new
privacy-infringing business-models and administrative practices. It explores how well the
existing legal framework is prepared for the future. Moreover, it provides an assessment of
available instruments which can be employed in making the responses.

The study takes into account not only technological developments (Chapter 2), but also socio-
economic (Chapter 3), administrative (Chapter 4), international (Chapter 5) and legal
elements (Chapter 6). In some cases, the focus is on specific technologies, but in general we
have applied a wider view in order to identify more general trends and developments.

The study pays due attention to the fact that some of the existing literature addresses concerns
that have been raised in legal and social contexts (notably the United States) that differ from
the European framework, but many of the challenges prevalent in the US are or should be of
concern to the European Union as well.

The study presents and explains possible responses to the challenges some of which have
already been discussed in the publications analysed in the preparatory collection and analysis
of existing literature. These responses (or measures) range from technical aspects to activities
of public administrations, from appropriate actions of private entities to legislative initiatives.
The emphasis is, however, on responses that the European Commission itself can take.

1.2 Privacy

Privacy is a complex construct that has received attention from researchers within a broad
spectrum of disciplines since the publication of Warren and Brandeis’s seminal publication in
1890.

For example, privacy researchers within the legal discipline argue that privacy should be
measured in terms of the rights of the individual whilst ethics researchers contend that the
morality of privacy protection mechanisms for the individual should be the focus of research
attention. Thus, it is necessary to examine privacy not as a single unambiguous concept but as
a class of multifaceted interests, a cluster of liberties, for instance, as a form of power, an
inherent right, an aspect of freedom or a psychological state.

3Friedewald, Michael, David Wright, Serge Gutwirth et al., Privacy and Trust in the Ubiquitous Information
Society: An annotated bibliography re privacy, trust and the Ubiquitous Information Society, Inception Report
(Deliverable 1), April 2008.
4But even within the legal discipline, there is considerable debate about the ways to comprehend privacy: some
argue that privacy is a right or a bundle of rights which implies a need for a definition, while others argue that
privacy protects individual autonomy and liberty, and thus should not be defined and remain contextual and
on p. 281; Acquisti, Alessandro, “Protecting Privacy with Economics: Economic Incentives for Preventive
For many researchers, the issue of control, more specifically the individual’s need to have control over his personal information, is a key aspect of the privacy debate.\(^6\) For example, Westin argues that privacy is the claim of individuals, groups or institutions to decipher for themselves when, how and to what extent their personal information is conveyed to others.\(^7\) This issue of personal control is also widely supported by researchers such as Fried who defines privacy as the “control we have over information about ourselves”\(^8\) and Parker who defines privacy in terms of the “control over who can sense us”.\(^9\) For Clarke, the significant importance of personal control lies in the fact that it relates to the interest of individuals to control or significantly influence the handling of their personal data.\(^10\)

However, the relevance of control as the central element of privacy is not undisputed. One can argue that this perspective is too narrow since not every loss or gain of control over information necessarily constitutes a loss or gain of privacy. For example, online users who voluntarily provide personal information in the course of their transactions may not view that as a loss of control and consequently as a loss of privacy. Even the knowledge that each of their online interactions is providing the vendor with a potential trail of information regarding who they are, their buying habits and other personal details does not necessarily constitute a lack of control or a loss of privacy in the eyes of such individuals. With that in mind, some researchers suggest that it would be better to focus on the issue of restricted access rather than on the individual’s need for control when trying to understand technology-related privacy issues.\(^11\)

Bohn et al. present a good overview of different aspects of privacy.\(^12\) First, they summarise different aspects of privacy:

- **Privacy as empowerment.** Seeing privacy mainly as informational privacy, its aim is to give people the power to control the publication and distribution of information about themselves.

- **Privacy as utility.** From the viewpoint of the person involved, privacy can be seen as a utility providing more or less effective protection against nuisances such as unsolicited phone calls or e-mails. This view follows a definition of privacy as “the right to be left alone”, where the focus is on minimising the amount of disturbance for the individual.

- **Privacy as dignity.** Dignity not only entails being free from unsubstantiated suspicion (for example, being the target of a wiretap, where the intrusion is usually not directly perceived as a disturbance), but also focuses on the equilibrium of information available between two people: as in a situation where you are having a conversation with a fully

---


dressed person when you yourself are naked, any relationship where there is a significant information imbalance will make it much more difficult for those with less information about the other to keep their composure.

- **Privacy as a regulating agent.** Privacy laws and moral norms can be seen as a tool for keeping checks and balances on the powers of a decision-making elite. By limiting information gathering of a certain type, crimes or moral norms pertaining to that type of information cannot be effectively controlled.

Second, they define what people perceive as borders protecting their privacy:

- **Natural borders.** Physical borders of observability, such as walls and doors, clothing, darkness, and sealed letters and phone conversations. Even facial expressions can represent a natural border against the true feelings of a person.

- **Social borders.** Expectations with regard to confidentiality in certain social groups, such as family members, doctors and lawyers. This also includes the expectation that your colleagues do not read personal fax messages addressed to you, or material that you leave lying around the photocopier.

- **Spatial or temporal borders.** The expectation by people that parts of their lives can exist in isolation from other parts, both temporally and spatially. For example, a previous wild adolescent phase should not have a lasting influence on the current life of a father of four, nor should an evening with friends in a bar influence his coexistence with work colleagues.

- **Borders due to ephemeral or transitory effects.** This describes what is best known as a “fleeting moment”, a spontaneous utterance or action that we hope will soon be forgotten, or old pictures and letters that we put out in our trash. Seeing audio or video recordings of such events subsequently, or observing someone sifting through our trash, would violate our expectations of being able to have information simply pass away unnoticed or forgotten.

Other works give more insight into the complexity of privacy. For example, Nissenbaum\(^\text{13}\) presents a model of informational privacy in terms of contextual integrity, namely, that determining privacy threats needs to take into account the nature of a situation or context: what is appropriate in one context can be a violation of privacy in another context. Nissenbaum also describes the connection between privacy and autonomy: the freedom from scrutiny and relative insularity are necessary conditions for formulating goals, values, conceptions of self, and principles of action because they provide freedom for people to formulate for themselves the reasons behind their choices, preferences and commitments. Thus, the privacy aspect called “utility”, the right to be left alone, is much more than just a utility because it is extremely important for personal development. This is what De Hert and Gutwirth call the negative and positive roles of privacy.\(^\text{14}\)

Singer argues that privacy is not only about disclosure of dangerous information or disturbing a person at a wrong time or with information on a wrong topic.\(^\text{15}\) For example, personalisation of advertisements may seem to be beneficial. Instead of a bunch of useless and time-robbing

---


advertisements about, e.g., new skis, a client who is not interested in skiing will receive advertisements about what he is truly interested in, for instance, new fishing rods. However, such personalised or targeted advertising is not so innocent or beneficial in the long term because advertising views people as bundles of desires to buy more and more, and this view is partially true. Precise advertisements are harmful because they proceed to reshape human nature to fit the picture of “being a bundle of desires”, diminishing people’s capacities of reasoned choice and thoughtful action. Thus, Singer’s work also links privacy to personal development.

1.3 PRIVACY AND DATA PROTECTION FROM A LEGAL PERSPECTIVE

Privacy is recognised as a right in different major international legal instruments. The Universal Declaration of Human Rights establishes it in Article 12. The International Covenant on Civil and Political Rights includes privacy in its Article 17. The European Convention of Human Rights (ECHR) recognises the right to privacy in its Article 8, whose scope seeks to protect four different areas of personal autonomy, not mutually exclusive: private life, family life, the home and one’s correspondence. The Charter of Fundamental Rights of the European Union explicitly recognises the right to privacy in Article 7, using the the same wording as Art. 8 ECHR.

The right to privacy protects the fundamental political values of democratic constitutional states as it guarantees individuals their freedom of self-determination, their right to be different and their autonomy to engage in relationships, their freedom of choice, their autonomy as regards their sexuality, health, social behaviour and so on. It guarantees each person’s uniqueness, including alternative behaviour and the resistance to power at a time when it clashes with other interests. By default, privacy prohibits interference by the state and private actors in the individual’s autonomy: it shields them from intrusions. The scope and reach of privacy are un(der)determined: it is up to the judges to decide when privacy interests are at stake and when their protection can rightfully be invoked. Legislators can also intervene to protect particular privacy interests, for example, through the enacting of professional secrets, the secrecy of communications or the inviolability of the home.

Art. 8 of the Charter of Fundamental Rights of the European Union recognises the fundamental right to the protection of personal data. The introduction of this article in the 2000 Charter has a long history: it was inspired by the Guidelines of the Organization of Economic Cooperation and Development governing the protection of privacy and transborder flows of personal data, the Convention for the Protection of Individuals with Regards to the Automatic Processing of Personal Data (“Convention 108”) of the Council of Europe and by EU legislation and more particularly by the EU Data Protection Directive. Data protection is both broader and more specific than the right to privacy. It is broader because data protection does not only aim at making concrete the protection of privacy, but also tends to protect other rights and interests such as freedom of expression, freedom of religion and conscience, the free flow of information and the principle of non-discrimination. It is more specific since it simply applies every time personal data are processed. The application of data protection rules does not require an answer to the question of the existence of a violation of privacy: data protection applies when the conditions put by the legislation are fulfilled. By default, data protection rules are not prohibitive, but they channel and control the way personal data are processed: such data can only be legitimately processed if some conditions pertaining to the transparency of the processing and the accountability of the data controller are met.
Even if they are intertwined and often overlap, and even if privacy is frequently used to mean data protection, the right to privacy and the right to data protection are separate fundamental rights, as has clearly been expressed in the Charter of Fundamental Rights of the European Union. As a consequence, this study on privacy and trust in the ubiquitous Information Society has not limited its scope to data protection issues (e.g., issues related to the processing of personal data) but has focused on all issues affecting privacy in the new environment. In this sense, it picks up the thread from Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector which, in order to protect privacy, provides for the protection of location and traffic data (which are not necessarily personal data). Indeed, privacy can be affected by the processing of non-personal data, such as traffic and location data, but also data concerning objects, movements, the detection of patterns and so on.

1.4 PRIVACY CHALLENGES

In general, invasions of privacy and improper use of personal information produce two kinds of risks, to the individual and to society. The UK Information Commissioner’s Office (ICO) concisely notes that societal harm can have multiple causes but improper use of personal information could be a significant factor in:

- excessive intrusion into private life which is widely seen as unacceptable;
- loss of personal autonomy or dignity;
- arbitrary decision-making about individuals, or their stigmatisation or exclusion;
- the growth of excessive organisational power;
- a climate of fear, suspicion or lack of trust.\footnote{16}

While economic growth in Europe is essential to individual and societal well-being, nevertheless, we must be attuned to the risks arising from the improper use of personal data, which fuel much of today’s modern service economy.

The surveillance society is already upon us.\footnote{17} There are thousands of surveillance cameras watching us, watching our every move, at least in London and, increasingly, in other places as well.\footnote{18} Not just outside in the street or in shops or on the metro, but also in our offices and at our workplaces.\footnote{19} Implants might become a requirement for those who work in critical

\footnote{16} UK Information Commissioner’s Office, \textit{Data Protection - Protecting People: A Data Protection Strategy for the Information Commissioner’s Office}, March 2008, pp. 7-8. \hspace{1cm} \url{http://www.ico.gov.uk/about_us/news_and_views/current_topics/data_protection_officer_conference.aspx}

\footnote{17} The theme of controlling and surveillance societies has received much attention since \textit{Surveiller et punir}, Foucault’s 1975 book on the 19th century’s disciplinary societies and their ‘panoptical’ institutions. His work has provided theoretical inspiration to many more recent works (for instance, of Stanley Cohen, Giles Deleuze, Gary Marx and David Garland) covering contemporary societies, and describing the development of control and surveillance strategies next to the disciplinary institutions. See Gutwirth, Serge, Privacy and the information age, op. cit., pp. 71-78. See also Wood, David, “Editorial: Foucault and Panopticism Revisited”, \textit{Surveillance \\& Society}, Vol. 1, No. 3, 2003, pp. 234-239. \url{http://www.surveillance-and-society.org}

\footnote{18} Samuel, Henry, “Paris to quadruple number of CCTV cameras”, \textit{The Telegraph}, 16 Oct 2008. \url{http://www.telegraph.co.uk/news/worldnews/europe/france/3209808/Paris-to-quadruple-number-of-CCTV-cameras.html}. The story quotes French president Nicolas Sarkozy as saying, “In my mind, there is no contradiction between respecting individual freedoms and the installation of cameras to protect everyone’s security.”

infrastructures. These phenomena are relatively well known. Perhaps less well known or so far contemplated are the implications of the convergence of the real and virtual worlds. Some companies are beginning to use virtual worlds, such as Second Life, for meetings, role-playing, training and so on as well as for advertising their wares. Will the day come when some people will be forced to have their own avatars (digitised graphical representations of themselves) because they work for a company which conducts role-playing or training or meetings in a virtual world? And how will crimes such as theft, stalking, slander or even murder be handled in such virtual worlds?

Various challenges mentioned in this study have not yet been discussed or scrutinised in academic journals, either because they are of relatively recent provenance (lead times for peer-reviewed publications are often up to two years) or we can see them at the very horizon of tomorrow. For example, the surveillance society has had a lot of media attention in the last few years, and that continues to be the case, especially in the context of governments, local authorities and law enforcement authorities watching what we do, but the media’s interest in personalised advertising and behavioural marketing is relatively recent, in the last year or so. As questionable as the surveillance society might be in general, the rise of targeted advertising is just as attention-worthy, if not more, because it is less visible than the cameras fitted to the interiors and exteriors of buildings and lamp posts in the streets and motorways but probably just as intrusive of citizens’ privacy. The biggest players and names on the Internet – Google, Microsoft, Yahoo and AOL – have been investing billions of dollars in new advertising technologies aimed at mining the data they capture from social networks (which they also own) and other sources to assess our interests and behaviours, the better to target us with adverts and to stimulate our buying proclivities. Some sociological and socio-psychological studies await an enterprising academic to assess the impact of highly targeting advertising bombarding us relentlessly whatever we do and wherever we go with our laptops, BlackBerries, mobile phones and other digital toys.

As another example, “social graph” is a (relatively) new buzz phrase in social networking. It means mapping everybody and how they are related. Industry is interested in the social graph, to discover with whom we network. Profiling users has become big business. However, it appears increasingly useful, for users, or more specifically, academics, privacy advocacy organisations and data protection authorities, to profile those who profile us, to discover and understand better the connections between those who seek to monetise our data. That is partly the purpose of section 3.5 of this report.

There is also a need to better understand the privacy implications of data portability – where personal profiles and associated personal data – can be ported from one social network to

---

23 These developments have recently been covered by popular scientific and journalistic publications, such as: Stross, Randall E., Planet Google: One Company’s Audacious Plan to Organize Everything We Know, Free Press, New York, 2008.
other websites – and third party applications, such as those written for social networks (Facebook reportedly has more than 20,000 third-party applications), some of which may trawl and repurpose personal data. Also important are the efforts and developments taking place in the private sector and within government or its agencies where (e.g., in Germany) there are numerous attempts to make different databases compatible or to merge them.

The erosion of privacy undermines our trust in government and in business. If people have minimal confidence that e-government and e-commerce will protect their personal data, then people will not use those services. Hence, we can say privacy is important not only to the individual but to society, the economy and the credibility of our political institutions. Privacy and trust are inextricably bound together, a point we emphasise in section 3.7.

Yet trust issues go beyond secrecy, seclusion and controlling information flows.

1.5 TRUST

Trust is something we deal with every day. We are expected to trust politicians to do the right thing and we demand our friends to be trustworthy when talking about private matters. In daily life, there are different definitions, which already seem to blur the concept of trust. Therefore, it is useful to see how social science has described the concept, for what purposes trust is important and how it is related to privacy.

First of all, trust is defined as a state between knowledge and nescience. In the original sense, trust means a kind of reliance between individuals. It is based on emotional bonds and is normally perceived as a positive experience. As trust is an important experience from infancy on, it becomes a vital part of human life. In daily life, however, people also trust people without this emotional quality. This is because human beings have to trust each other to some extent, otherwise daily life would be impossible. Because of the number of people involved in our daily life, we have to rely on “stressable” conditions established by society. Here, a distinction between trust and confidence comes into play. In contrast to trust, which applies only to interactive situations between people, confidence is a more abstract phenomenon.

Digital technology increasingly mediates between people and the world. Such technologies structure, constrain and enable our engagement with and experience of the world. Simply said, our life is increasingly intertwined with or related to digital technology. In order to put digital technologies to satisfactory use, and in order to have a convenient and useful interaction with and through technology, trust is a fundamental precondition.

Traditionally, the issue of trust in computers involves security and development of safer and more dependable (“trustworthy”) systems. While the technical security approach is not to be discounted, especially in high-risk system implementations, focusing exclusively on technical solutions to the challenges of trust is not adequate in increasingly digitalised environments.

A precursor of trust is the assumption of risk. Hazards abound in late-modern society, are fundamentally changing and deepening our need for trust. Had we not trust in much of the apparatus of late modern society, we would not be able to act at all, we would be in fear of venturing out into a society permeated by seemingly inescapable danger. Trust can be

---

conceptualised as “a willingness to enter into interaction under the face of uncertainty”.26 Trust, then, is an active stance, as opposed to background human phenomena such as confidence or faith. If trust is not reciprocated or turns out to be imprudently given, we regret our action of having extended trust. If confidence results in disappointment, we cannot but ascribe this to bad luck. Trust, then, is an assumption of others’ competence or benign nature, while disappointed confidence will be ascribed to external factors, not something intrinsic to an interaction partner, whom we may still trust.27 Thus, trust has to do with the experience of actors and acting rather than factors. Trust can be strategically managed at a social level, while confidence works as an ambient background premise.

In his theory of trust, Niklas Luhmann stresses the importance of trust for the reduction of experienced risk in complex environments, and the accompanied increase of possibilities for experience and action when we do trust. Trust, in Luhmann’s conception, is a feature of a relation that “brackets” external uncertainty and replaces this with an internal experience of certainty, allowing for continued interaction. According to Luhmann, by trusting we accept our own and others’ limitations in predicting the future, especially as the future is structured by the freedom of others to act as they see fit. Trust, then, as a reducer of societal complexity is different from security obtained through political, judicial or economic domination. Indeed, trust, and not necessarily objective security, becomes an increasingly important strategy in highly complex societies, where the outcomes of actions are, and are experienced to be, highly contingent and hence highly risky and where the scope for action and interaction is extensive. This also means that trust is no static construct but a highly dynamic process where the premises of trust are constantly monitored and reassessed. This does not only occur on a rational level but also includes weak factors like our attitude towards technological solutions or the subjective perception of the situation (see figure 1). It is hence not enough to implement trustworthy technological solutions; they also have to be embedded in a socially and organisationally trustworthy way.

Figure 1: Trust-building process

Further, trust as a strategy for coping with social complexity means a necessary departure from traditional forms of social contracts such as familiarity. Given the speed with which new technologies emerge, pervade into and change our lives, and given the complexity already inherent in technology and social structure, we cannot relegate our engagement with the world to familiarity, as that which is familiar today may be estranged or change its status tomorrow, due to new insights and new knowledge. Late-modern society is one of reflexivity and radical scepticism towards claims of essentialist truths and objectivity.\textsuperscript{28}

There is a complex interplay between privacy and trust that is of importance for this study. On the one side, privacy is an important factor in the trust-building process. If the user has a negative feeling about the possibility of ICT systems to invade privacy or if one feels that the risk resulting from the disclosure of personal data is not acceptable, this will affect the trust in the system adversely. More important for the purpose of this study is the reverse effect. If users do not trust in privacy-enhancing solutions (for instance, because it is not transparent for the user what happens with his personal data inside the technical solution), one may prefer to use simpler, but potentially more privacy-violating solutions.

1.6 **Examples of key privacy and trust issues**

Data integrity and authenticity are of utmost importance, as novel forms of identity theft and viral marketing demonstrate: How should I react if others can use and abuse my data as their own? How should I react if the single mother on my favourite online bulletin board turns out to be not a mother of three living in the south of Germany, but a temp at a Berlin ad agency hired by the brand manager of the product she is recommending? Just as we are beginning to understand how easily digital photography can be used to manipulate images (as the Reuters photographer did when he added extra smoke to the sky of Beirut in 2006\textsuperscript{29}), we might have to learn the same for digital profiles, which can just as easily be cut, amended or changed to paint a convincing picture of one’s life.\textsuperscript{30}

Cybercrime, also addressed in this report, is hardly a new phenomenon and so one might question why it should be included in a study on emerging challenges to privacy and trust in the ubiquitous information society. Two reasons stand out – first, cybercrime continues to be a problem, even a growing problem, so it means more effort is needed to contain it and, second, new forms of cybercrime are emerging all the time.

We also need some way of measuring how successful privacy protection is or has been, some metrics that would address, for example, the following:

- How many enforcement actions have been taken by data protection authorities?
- How many successful prosecutions have there been?
- How much have offenders been fined or otherwise penalised?
- From what sectors have offenders come?
- What initiatives have data protection authorities taken to inform the public (data subjects) and data controllers about the arcana of data protection law?


\textsuperscript{29} http://en.wikipedia.org/wiki/Adnan_Hajj_photographs_controversy

It would probably be useful to assess what differences there are across countries in how privacy is understood. Or, as a minimum, how the Data Protection Directive, e-Privacy and Data Retention Directives have been implemented in the Member States. What might be seen as a challenge to privacy in the UK might not be seen as an issue in Bulgaria.

1.7 STRUCTURE AND METHODOLOGY & CRITERIA OF THE STUDY

This report is organised in two main parts: The first one deals with the identification and analysis of challenges and the second with possible policy responses.

The general approach followed in preparing the first part has been to identify challenges to privacy and trust from technological developments (Chapter 2), socio-economic developments (Chapter 3), administrative developments (Chapter 4) and international issues (Chapter 5). Chapter 6 addresses legal challenges, while Chapter 7 summarises the main, cross-cutting challenges, i.e., those that recur across different developments.

The identification of privacy and trust issues (challenges) raised by the ubiquitous Information Society was based on a rather exhaustive sweep and compilation of documents dealing with privacy and trust issues. These documents came from all major sources dealing with policy, legal and regulatory aspects of new technologies:

- Articles from major academic journals in the field of science, technology and law studies, data security and data protection as well as ubiquitous technology,
- Press stories from major news media,
- Reports and studies from the European Technology Assessment community
- Legislative, regulatory and policy documents, including documents from all relevant European institutions and their working groups dealing with privacy issues.

The issues and challenges addressed in those documents were clustered in a systematic way using a taxonomy based on those put forward by Daniel Solove and James Waldo et al., which is reflected in the structure of Chapters 2 to 6. While the taxonomy in general aims to be as generic as possible to provide a broad view of privacy issues, in some instances, we have focused on specific technologies.

The importance of the challenges has been assessed in a partly objective and partly subjective way. The criteria used for this assessment include the following:

- The probability that a challenge (risk) becomes reality. For instance, one of the fears regarding RFID is that tags can be read secretly and remotely at a distance. However, this is a rather unlikely type of attack because the necessary technical effort is much higher than that for other kinds of attacks.
- The domain and size of the affected group (single persons, broad public, certain groups in society, certain industry sectors).
- The extent of harm related to a certain privacy challenge. This includes not only quantifiable (economic) factors but also soft factors like fairness, trust in government and democracy.

31 The analysis of documents was mainly finished by September 2008. New developments that were brought to our attention after that date could not be taken into account systematically.
Apart from these three criteria, there were other factors taken into account:

- Which challenges are developing most dynamically?
- Which challenges are little noticed by the public and policy-makers though having a big impact?
- Which challenges are not already addressed by existing laws and other instruments?

As a result of the clustering and assessment process, we have identified challenges at two levels of detail. First, Chapters 2 to 6 present concrete challenges, i.e., challenges that are the result of the use of a specific technology for a specific application. The construction of movement profiles for tolling and road pricing purposes is an example of this type of challenge. In Chapter 7, however, we summarise the numerous privacy challenges at a higher level, because there are numerous examples of profiles that can be built using ubiquitous information technology. This generalisation makes clear where we do not face a simple extension of the possibilities of today’s technology but where we cross a border that marks a paradigm shift in the way information is used in society and economy.

The second part of the study deals with possible responses to privacy and trust challenges. In describing many of these challenges in the first part of the report, we indicated some possible responses. In Chapter 8, we have collated and summarised these responses and grouped them as technical responses, administrative responses, awareness-raising and education measures, self-regulation and other measures, and legal responses. The responses can be made by different stakeholders, but especially the European Commission. Chapter 9 outlines various instruments at the disposition of the Commission by means of which it can undertake responses. In Chapter 10, we define criteria for assessing response measures and use them to assess the response measures and responses to the challenges as summarised in Chapter 7. Finally, we draw our conclusions from this study in Chapter 11.
2 CHALLENGES FROM TECHNOLOGICAL DEVELOPMENTS

Ron Rivest, professor of Electrical Engineering and Computer Science at the Massachusetts Institute of Technology, once described the outlook on information technology as a “reversal of defaults”: “What was once private is now public”, “what was once hard to copy is now trivial to duplicate” and “what was once easily forgotten is now stored forever.”\(^{32}\) This chapter depicts trends in technology and applications that have privacy and trust implications for the ubiquitous Information Society – trends that point toward a future where storage is so cheap that deleting data will be more costly than keeping it, where online connectivity will be fast and ubiquitous so that “always online” will be the norm, where information flows constantly and where countless sensors will be able to record and interpret our actions, physical conditions and even thoughts.

The technologies described below are either already existing or will be deployed soon. We have purposefully restricted our analysis to near-term developments that already pose challenges to our current notions of privacy and trust, notwithstanding future technology shifts that might further push us towards Rivest’s future.

The technologies and applications have been grouped according to their (technological) function, roughly following the data processing cycle: from information collection technologies to communication technology, and from information exchange technologies to storage and processing (see Figure 2 below). However, this technology-centric view is by definition incomplete – it is often only the application of technology that determines whether it is beneficial or detrimental to our physical and psychological well-being. As Melvin Kranzberg notes in his First Law of Technology, “Technology is neither good nor bad. Nor is it neutral.”\(^{33}\) The discussions in this chapter attempt to explore this lack of neutrality in current and future technology developments.

\[\text{Figure 2: A simple grouping of technological developments that have privacy and trust implications. Note that these must be closely linked to applications.}\]


2.1 INFORMATION COLLECTION TECHNOLOGIES

Advances in technology allow for an ever more precise and ever cheaper way of identifying things and people. The following three types of technologies can be considered information collection technologies, as they simplify and automate the collection of personal data (and identifiable data): positioning and tracking technologies, identification technologies, and activity and ability recognition technologies.

2.1.1 Positioning and tracking technologies

Novel positioning technologies allow us to more often and more precisely know where you are. Knowing where you are often allows one to infer activity, by virtue of a place (e.g., if you are in a supermarket, you might be doing your groceries). Identification is also possible by means of data fusion, e.g., correlating phone book data and location traces (see section 2.4 on information processing below). With additional personal information, activity inference can further be refined (e.g., if you work as a supermarket manager, you might not be shopping when in a supermarket but actually working).

Positioning technologies

Positioning technologies can be subdivided into two categories for the purpose of a privacy analysis: self-positioning and remote positioning. Self-positioning systems support an infrastructure that supplies users with enough information to independently deduce their current position, i.e., without transmitting any information back to the infrastructure. Good examples are outdoor positioning systems such as GPS or the planned Galileo navigation satellite system, but also Microsoft’s FM-based RightSPOT system\(^{34}\). Several indoor-location systems such as MIT’s Cricket\(^{35}\) or Hazas’ and Ward’s broadband ultrasonic system\(^{36}\) have been specifically designed with self-positioning in mind. They have, however, not yet found widespread commercial use.

Some wireless communication technologies, such as GSM and UMTS, as well as Wi-Fi, Bluetooth, ZigBee, or Wireless USB, could in principle also support self-positioning, since they only require a signal-strength measurement on the client side, together with a properly calibrated lookup table. In practice, however, these are typically combined with regular communication traffic (e.g., using a mobile phone for calling, or providing Internet connectivity on a laptop), thus implicitly allowing third parties to infer the user’s location through the currently used access point or cell tower.

Remote positioning systems require the infrastructure to locate the device (e.g., to perform time-of-flight measurements), thus inherently sharing this location with the service provider.


Examples for such systems are UWB\textsuperscript{37} and ultrasound systems such as the ActiveBat\textsuperscript{38}. However, as such systems are typically costly to install, their use is restricted to selected indoor applications, e.g., for head tracking in research and gaming, or in industrial environments (e.g., locating containers in storage facilities).

In some countries, especially the United States, operators are required to collect location information so they can pass this on to the emergency services when needed (“E911”). The cost of compliance with such directives can be a burden on mobile networks, especially as regulations demand ever-greater accuracy. The development of Assisted GPS (A-GPS), which combines satellite and cell-site data with remote processing to give more accurate positioning information, especially in urban canyons where GPS signals can be hard to pick up, promise lower cost and improved reliability. A-GPS is increasingly integrated in mobile handsets (e.g., the Nokia N95). Qualcomm has shipped more than 300 million handsets with A-GPS. Such location technology – combined with free navigation and mapping tools, where Google Maps is currently the leader – leads to the diffusion and wide use of location services. The adoption of tracking services such as “geo-tagging” and “geo-fencing” is expected to further increase for individuals and businesses.\textsuperscript{39}

Identification technology such as RFID readers, biometric scanners (e.g., fingerprint or iris scanners) and/or smart card readers also allow the localisation of identified persons, as the position of the device reader is known. This becomes particularly relevant as the density of both readers and identifiable objects (e.g., RFID-tagged items) increases, again due to falling costs. In this manner, such systems act as remote positioning systems.

**Location privacy**

Of particular importance in a location system is not only how the positioning information is acquired, but maybe even more how it is used. As long as GPS signals are simply used to locally compute a route based on a known map, no positioning information is exchanged with any third party. Using the same GPS data, however, to query a server for best gasoline prices in the vicinity will lose most of the anonymity advantages of the self-positioning approach. In this respect, it is thus not only important to look at the act of positioning itself, but also at the use and storage of such data by third parties.

As soon as positioning data are sent to a server in exchange for a service (e.g., providing location-based recommendations, or allowing friends and family to find out where one is), these data can be mined for information, especially when long-term data are available. Many researchers have demonstrated how to deduce one’s “important places” (e.g., work, home) from pseudonymised GPS location tracks. Recent work has even successfully mined fully anonymised location data, i.e., without any identifiers attached. This makes use of military multi-target tracking algorithms and is thus able to sort all data points into coherent trajectories, which can then be used just as pseudonymised location tracks.

\textsuperscript{37} See, e.g., \url{http://www.ubisense.net/}
To protect against such privacy invasions, researchers have looked at obfuscation techniques that hide the user’s true position, e.g., by introducing a random co-ordinate offset or clipping a position to a large grid, e.g., 1 x 1 km. However, as Krumm has demonstrated, even such imprecise data points can be used reasonably well to infer one’s “important places” with high probability. It also remains questionable if users are willing to tolerate a degradation in the performance of their location-based services due to such obfuscated positioning data.\(^{40}\) Other researchers have proposed the use of dummy traffic, in which the real user’s position would be hidden. Such an approach is only possible in self-positioning systems, or if the entity offering the service is different from the one doing the positioning. Such dummy traffic would need to be carefully engineered in order to make all reported positions look valid. Also, in order to prevent a single identified disclosure (e.g., the use of a personal credit card in a shop) to reveal the entire “true” track, such dummy tracks need to frequently intersect the user’s true track. In this way, both the location history and future movements would branch off quickly into many possible tracks. While a formidable technical challenge in itself, no economic analysis of such an approach has been undertaken yet, as the location and service requests from all those “dummy users” might amount to significant costs.

Even “dumb” (passive) sensors like motion detectors or pressure sensors in floor mats can be used to discern movement patterns from a selected set of known users.

A significant amount of work is being done on supporting k-anonymous\(^{41}\) queries in location-based systems, i.e., hiding a particular user request among k-1 other potential users in the vicinity so that an attacker would not be able to distinguish between k sources of the request.\(^{42}\) Note that such attempts are not actually about location privacy, but concern information privacy, i.e., hiding the identity of a requestor, rather than his or her location: If sent from within a crowded subway train in downtown Tokyo, even large values of k would allow for a very precise tracking of a person’s location.

**Verifiable location claims**

Location information can also be used to increase consumer trust and security. The idea is to use spatial constraints to limit access to information, instead of allowing remote queries from anywhere in cyberspace. Examples would be to limit access to your health record from within your doctor’s office, or to require physical presence in your own home in order to open your personal financial records.\(^ {43}\)

---


Challenges

With the increasing availability of cheap and miniature localisation technology, a number of privacy-related challenges may arise, notably

- Who should have rightful access to location data – the person being located, the owner of the devices that enable the localisation (e.g., the car she is driving), or anybody in the vicinity?
- How can consumers be educated about the dangers of publishing location information about themselves, in order to make informed choices about what location-based services to subscribe to, or with whom to share their current location (e.g., publishing it on their social networking site)?
- Are consumers able to configure the disclosure policies of their personal positioning technology (and of any devices that they rent or borrow) so that it conforms to their interests?
- What legal requirements should there be regarding the process of fusing multiple position reports, also from different devices and owners, together in order to derive detailed movement profiles?
- How should the location privacy of minors be balanced against the desire of parents to know where their children are? What about employees and employers? Can children and employees be forced to be locatable?

2.1.2 Identification technologies

Identification technology addresses questions such as “Who are you?” but also “What are you carrying?” Any identification usually entails positioning, i.e., the fact that you are identified also yields information about where and when this is happening. Even anonymous identification of things might encroach on one’s privacy, e.g., through social sorting (people with this kind of clothing are not potential customers) or the disclosure of facts (brand of underwear I’m currently wearing, or even how long I have been wearing it). A few examples of popular identification technology are:

- radio frequency identification systems (RFID), both active and passive,
- mobile payment systems based on RFID or other short range communication technology, such as NFC, Bluetooth or ZigBee,
- biometric identification systems based on iris scans, fingerprinting, gait analysis, typing patterns or even DNA analysis.

Current trends in identification technology attempt not only to increase identification rates (while lowering rates of false positives and false negatives), but also to improve identification speed and the overall process. In particular, technology such as RFID or face recognition allows identification from a distance, i.e., without the help or even the knowledge of the identified subject. Furthermore, some of the new identification mechanisms allow for automated identification that can be done solely by the computer without the aid of a person.
Radio frequency identification

A number of background articles provide a good overview on RFID technology. RFID tags can be categorised into two classes: active and passive, depending on their power source. Passive RFID tags do not possess their own power supply – the reader supplies the tags with power through the coupling unit along with data and clock pulses. Active RFID tags, on the other hand, feature a battery in order to extend their transmission range and reliability. While future applications in the mass consumer market, e.g., supermarket item-level tagging, focus predominantly on the use of passive tags, active tags continue to play an important role in many closed-loop supply-chain scenarios, e.g., container tracking. The use of RFID as part of electronic toll gates is also based on active RFID technology. Current research in passive RFID technology is mostly concerned with commoditising chip production, e.g., by printing entire tags directly on their substrate, instead of using costly chip assembly processes.

Most of today’s privacy concerns focus on applications utilising passive RFID tags: smart checkouts in supermarkets through tagged merchandise; human identification through tag injections under the skin; RFID-tagged banknotes, medical drugs or luxury goods for preventing counterfeiting; or passports with embedded tags for the secure storage of biometric data. The main problem is not the lack of adequate levels of encryption strength (though it remains challenging to offer this for ultra low-cost tags), but rather the difficulty of managing this additional security infrastructure, especially in consumer applications. Solutions need to scale to hundreds of tagged items per person that often change ownership, sometimes without the availability of additional infrastructure (such as checkout terminals). The use of password-less encryption methods seems promising, yet is still far from being deployable.

Mobile payment

One increasingly popular consumer application for RFID is mobile payment. RFID-enabled credit cards are already widely deployed in the United States and other countries (e.g., American Express ExpressPay, Mastercard PayPass). According to Visa USA, an estimated 20 million RFID credit cards and 150,000 vendor readers were already deployed in the US by 2006. Using samples from a variety of RFID-enabled credit cards, an independent study by Heydt-Benjamin et al. observed that the cardholder’s name and often credit card number and expiration date are leaked in plaintext to unauthenticated readers. The credit cards examined were ISO 14443-B cards with a nominal range of 4 to 5 centimetres. Vendors and credit card companies have so far been reluctant to recognise the deficiencies of the technologies employed.

---


Traditional smartcard-based payment systems, notably the EMV payment protocol, promises better security through more advanced encryption capabilities, but even those systems have proven vulnerable to attacks. In 2006, following the discovery of a systematic fraud that resulted in the theft of £1 million from customer accounts, Shell stopped accepting EMV payments (called “Chip and PIN” in the UK) at 600 out of 1,000 UK petrol stations. In contrast to traditional credit card payments, customers with EMV cards are liable for fraudulent transactions: the security of the protocol makes it practically impossible to use EMV-based cards without its owner disclosing the secret PIN. However, thieves can often easily observe consumers entering their PIN in public terminals (e.g., when buying a train ticket), then attempt to steal the card and, if successful, withdraw large amounts. A thief in Switzerland was able to withdraw over SFr. 37,000 in this manner.49

Already in widespread deployment are contactless payment systems in transport, e.g., the Oyster Card in London, the SUICA and PASMO systems in Japan, and the Octopus card in Hong Kong, all based on the ISO/IEC 14443 standard for proximity identification cards. Several mobile phones offer integrated payment cards, which allow their owners to enter subway turnstiles or buy from vending machines simply by waving their phone.

The overall trend in mobile payment is to significantly increase its share in small transactions, i.e., involving a few euro. While credit cards have traditionally been used for large-scale payments such as flight tickets or hotel rooms, the extension of electronically traceable payments to subway or parking tickets, sales of chewing gums or soft drink cans casts an ever wider net on each individual’s movements. While payment schemes exist that provide unconditional anonymity, such as Proton, eCash or the CAFE payment system, these electronic payment systems have not been used on a large scale yet, as governments and banks do not accept them.

**Biometric identification**

Biometrics are a convenient way to identify and authenticate individuals. The identification process consists of the comparison of live anatomical, physiological or behaviour characteristics to equivalent, stored information. Depending on the kind of information they use, biometric technologies are mainly divided into two categories: *physiological* (based on fingerprints, hand and/or finger geometry, and the patterns of retinas, veins, irises, DNA and faces, etc.) and *behavioural* (based on voice, signature and typing behaviour). Many other biometric systems, such as the recognition of a person’s earlobe, ear shape, smell, gait and pressure with which keys are pressed, have also been proposed but are not yet reliable. Furthermore, techniques such as recognition of laughter, bones in the finger, facial thermograms, inner ear bones and lip shape have been discussed recently, but many of them are unfeasible or still in a very incipient phase.50

A recent development is the increasing use of biometric identification in the context of video surveillance, i.e., in the form of automated face recognition. Several US airports have adopted

---

such systems in the wake of the 11 September 2001 attacks; also much publicised was the use of this technology at the 2001 Super Bowl in Tampa, Florida. A large-scale trial in Germany with more than 200 volunteers has been underway since 2006, where a system was installed in the main station of the city of Mainz. Most systems still struggle with relatively high false positive rates, rendering them impractical in any large deployment due to the many false alarms they trigger. Three-dimensional face recognition has recently been demonstrated as a viable alternative, as it allows for much better detection rates.\footnote{Bronstein, Alexander M., Michael M. Bronstein and Ron Kimmel, “Expression-Invariant 3D Face Recognition” in Josef Kittler and Mark S. Nixon, *Audio- and Video-Based Biometric Person Authentication*, 4th International Conference, AVBPA 2003 Guildford, UK, 9-11 June 2003 Proceedings, Springer LNCS 2688, 2008, pp. 62-70.}

One major security issue with the use of biometrics is the storage of reference data, the so-called templates. Biometric templates are basically processed measurement data and are typically represented as feature vectors in a high-dimensional space. The disclosure of such templates significantly affects the template owner, since biometric data, unlike passwords, cannot be changed. Recent stories of lost government laptops highlight the fact that template disclosure can happen quickly. Several techniques are currently available to protect stored template data, such as *cancellable biometrics* or *fuzzy vaults*\footnote{Coventry, Lynne, *Usable Biometrics in Security and Usability: Designing systems that people can use*, O’Reilly Media Inc., 2005.}.

**Challenges**

Among the main challenges arising from identification technologies are these:

- Are RFID users aware of what maintainers can and are allowed to do with RFID data?
- How can one assess the linkability of an RFID reading to its owner? Can we define a measure for this that can be used to require minimal anonymity levels?
- How can one ensure that adequate security safeguards are in place whenever biometric access control systems are deployed?
- Should the proliferation of biometric access control systems be curbed or encouraged? What are the implications of widespread biometric identification systems?
- How will the error rate of biometric identification systems affect consumer trust due to misidentifications leading to denied service (e.g., boarding an airplane)?
- How will the move to mobile and fully digital payment systems (i.e., signature-less, PIN-based) affect fraud and thus consumer trust?
- How will data breaches (e.g., stolen laptops with corporate or governmental databases) involving biometric templates affect biometric access control systems? Can victims of such thefts become “non-authenticatable” in biometric systems as their identifiers have become public knowledge?

**2.1.3 Activity and ability recognition**

Novel sensors and algorithms allow us to infer human activity and ability, i.e., to answer questions such as “What are you doing?” and “What are you thinking?”. The example technologies below usually entail a place, by virtue of where the sensing was done (e.g., which access point was used). However, the use of pattern recognition software or sensors usually yields additional information (e.g., whether you are in a parking lot looking for your car or a car to break into). Biometric identification and novel (bio)sensors might also disclose
information about one’s personal physical and mental wellness (“How are you feeling?”). Among the new recognition technologies are the following:

- smart CCTV (with image and/or facial recognition), spy drones, etc.,
- brain-wave scanning, brain “fingerprinting” (especially in connection with the proliferation of brain-computer interfaces),
- DNA profiling (identifying individual social predispositions),
- the monitoring capabilities of computers, mobile phones, smart homes, ISPs.

**Smart CCTV**

As described in the preceding section, smart CCTV systems with automated facial recognition already allow for the unsupervised operation of large-scale people searches. Automated activity recognition systems such as the IBM’s S3 system\(^53\) enable the detection of unusual activity in video images, alerting service personnel to suspicious people in a car park or forming crowds. Once CCTV systems are interlinked, comprehensive activity and movement profiles can be captured, as demonstrated by the UK roads policing strategy which connects existing CCTV cameras along all major UK highways with the city cameras supporting the London congestion charge system and with number plate recognition software employed to comprehensively “deny criminals the use of roads”.\(^54\)

MIT professor emeritus Gary Marx calls such systems the “new” surveillance, as they are less visible and more continuous in time and space, provide fewer opportunities for targets to object to or to prevent the surveillance, are greater in analytical power, are disseminated faster and more widely, and are less expensive than the “old” surveillance techniques.\(^55\)

**Brain and DNA fingerprinting**

Brain “fingerprinting” is the process of detecting instrumentally whether certain information is stored in the brain of an individual being tested, or whether particular thoughts are forming. A brain-computer interface (BCI), sometimes called a direct neural interface or a brain-machine interface, is a direct communication pathway between a human or animal brain (or brain cell culture) and an external device.\(^56\) In one-way BCIs, computers either accept commands from the brain or send signals to it (for example, to restore vision), but not both. Two-way BCIs would allow brains and external devices to exchange information in both directions but have yet to be successfully implanted in animals or humans. Technological advances have come as far as allowing humans to control telepathically a robotic arm just by thinking about moving one’s hand and, with the use of a computer cursor, lights and TV.\(^57\)

By capturing electronic impulses sent by the brain with the help of a neckband, scientists from Ambient Corporation, Dallas, have recently achieved the transformation of thoughts into

---


speech (although at the moment only around 150 words and phrases can be recognised). In 2007, scientists from the Max Planck Institute for Human Cognitive and Brain Sciences in Leipzig claimed that they could “read minds” and predict what a person is about to do. For this, they use sophisticated functional magnetic imaging (fMRI) and computer programs.

A similar predictive ability, albeit with a much longer reach, is promised through DNA analysis. Using DNA profiling – not for identifying subjects or acquitting suspects, but to search for genetic predispositions towards violence, child molestation or terrorism – might allow law enforcement authorities not only to react to crime but also to predict it. If it can be predicted, so the reasoning goes, it could be prevented, as depicted in the Steven Spielberg film Minority Report.

Biology has advanced today to the degree of being able to read genetic predispositions towards both diseases and psychological traits through DNA tests. While the benefits of knowing in advance and thus preventing special conditions are considerable, the potential discrimination by future employers and health insurance companies raise serious privacy concerns. As a consequence, many citizens are fearful of having their DNA tested, as information from such tests might find their way to future employers or insurance companies. Several companies in the US are profiting from this by offering private DNA testing, e.g., the start-up company DNA Direct.

Detecting activity through search engines

The information that we disclose while using search engines or simply the services of our Internet service provider can be used to form a clear picture of our personal and professional lives, current activities and interests, as discussed later in section 3.1.1 on behavioural advertising. Security measures such as encryption and firewalls are inappropriate due to the implicit trust paradigm with the service provider. In his paper “Googling considered harmful”, Gregory Conti raised awareness about the practices of ISPs and search engines in collecting enormous amounts of data about individuals, an issue which is discussed further in this report, especially in section 3.1.1 and section 3.5 on the convergence of companies.

Aggregating detected activities, fingerprinting and tying them to real world personas often with the use of IP addresses, geo-localisation data, etc., represent real privacy threats. In addition, advanced technologies such as data mining, artificial intelligence, genetic algorithms, information retrieval, machine learning, natural language processing and profiling provide the capability to deeply explore and interconnect the data. See also section 2.4 below.

Challenges

Among the main challenges arising from activity recognition technologies are these:

- How should we handle “side-channel” information, e.g., information about a tendency for child molestation gleaned from a biometric identification system?
- Will brain fingerprinting become a required access control mechanism, in order to ensure that a person does not plan an attack?
- How should we draw a line on the use of activity collection and location tracking that becomes possible with integrated CCTV systems? Should, in general, everything be linked that can be linked?
- How can consumers be educated about the implications of their online behaviour, in particular their online searches?

2.2 COMMUNICATION AND DISSEMINATION TECHNOLOGIES

Communication technology does not provide data collection options per se, but it significantly lowers the cost to disseminate and process personal information. It thus enables an unprecedented digitalisation of everyday activity (which in turn then allows inference of activity, social relationships, location, etc). Two recent developments are notable and have a great impact: (1) the comprehensive availability of wireless communication technology across any distance, far and near, and (2) the decreased data transmission cost. Of special interest are wireless communication technologies, as they offer data collection anywhere, anytime:

- Body area networks, personal area networks,
- Wi-Fi, WiMAX, Wireless USB, ZigBee, UMTS/3G,
- Internet of things,
- IPv6, MobileIP.

Communication technologies have evolved to a great extent in the last few years. They now cover the full communication spectrum, from short-range like Bluetooth and ZigBee, up to UMTS 3G and WiMAX standards. Short-range communications are combined with higher range technologies (e.g., Wi-Fi) to create Personal Area Networks (PAN) or to collect and transmit medical information in Body Area Networks (BAN). At the other end of the spectrum, long-range technologies play a key role in the developments of Wide Area Networks (WAN) and Metropolitan Area Networks (MAN).

The increase in capacity and availability of such technologies, on the one hand, and the falling hardware and communications cost, on the other, push towards the ubiquitous vision of connectivity, soon making it possible for anybody to access and transmit large amounts of information anywhere and at practically no cost. In this section, we present the state of the art in communication technology standards in terms of transmission throughput, range and cost.
Even if the content of communication is not stored, the recording of communications data allows the construction of detailed personal communication patterns and even mobility patterns if GSM/UMTS cell information is available.

The basis for most of the technologies described below is the availability of cheap broadband access. In many countries, citizens can connect their homes with tens of megabits to the Internet, using either DSL/ADSL or TV cable. The abundance of fibre has seen prices erode significantly in recent years. See also section 3.2.2 on IPTV and broadband convergence.

**Wireless communication technologies**

A range of novel wireless communication technologies allow for an ever denser and increasingly cheaper level of connectivity.

Wi-Fi has become a very popular technology for wireless communication with wide deployment in homes, offices and even in cities, e.g., through hot-spots. It is supported by most modern computers, mobile devices, etc. Computers can be enhanced with Wi-Fi capabilities through the widely available USB devices, which offer a compact design and cost as little as $20 (e.g., Netgear RangeMax 802.11g Wireless USB 2.0 Adapter on Amazon). Wireless cards for PDAs are also available (e.g., SPECTEC SDIO Wireless LAN Networking Card WLAN 802.11b costs about $65 on Amazon). By acquiring and installing a wireless router, anyone can create a Wireless Local Area Network (WAN) for home or office. The choice of devices is very broad, with different specifications and designs, costing from $40 (4-Port 802.11g 54Mbit/s Wireless Broadband Router) up to $300 (7 dBi Omni/Directional Rubber Duck Antenna Wireless b + g Router) or more.

Wi-Fi is based on the family of IEEE 802.11 standards, which vary in range and throughput. A typical Wi-Fi home router using 802.11b or 802.11g might have a range of 32 m (120 ft) indoors and 95 m (300 ft) outdoors and a throughput of 54 Mbit/s, which, however, decays fast with distance. Both 802.11b and 802.11g standards operate in the 2.4 GHz frequency band, which provides better performance than the previous 802.11a at 5 GHz.

The next Wi-Fi standard, IEEE 802.11n, is scheduled to be released in June 2009. It is the first wireless LAN standard based on multiple input, multiple output, orthogonal frequency-division multiplexing (MIMO-OFDM), a technique which gives a significant performance increase in both range and transmission rate compared to conventional wireless LAN. As van Nee et al. describe it, “performance results show that net user throughputs over 100 Mbit/s are achievable, which is about four times larger than the maximum achievable throughput using IEEE 802.11a/g. For the same throughput, MIMO-OFDM achieves a range that is about 3 times larger than non-MIMO systems.”

The availability of broadband wired access and inexpensive wireless routers has significantly affected information availability and communication capabilities. All modern laptops have built-in Wi-Fi which allows their owners to be online in airports (soon also in airplanes), train stations (and increasingly trains), cafes and hotels – usually for a small fee but often for free.

---


Recent mobile phones not only feature GSM/UMTS and GPS, but also a Wi-Fi receiver for cheap and fast large-volume data transfer. While security awareness has significantly increased in recent years, many “hotspots” are still left unsecured or use outdated security standards (i.e., WEP), while consumers often transmit sensitive information over unsecured connections (making a Starbucks an ideal place for stealing logins and passwords).

WiMAX\(^{67}\) (Worldwide Interoperability and Microwave Access) provides wireless connectivity over long distances, closing the gap between popular Wi-Fi medium range communication and mobile phone technologies such as UMTS. WiMAX is “a standards-based technology enabling the delivery of last mile wireless broadband access as an alternative to cable and DSL”, says the industry-based WiMAX Forum.\(^{68}\) Connectivity is achieved through a variety of methods, from point-to-point links to full mobile cellular type access. WiMAX is based on the IEEE 802.16 standard, which is also called WirelessMAN (for “Metropolitan Area Network”). With its high-speed data and connectivity, WiMAX will play an important role in creating the so-called Internet of things. It can be used to connect Wi-Fi hotspots with each other and to other parts of the Internet. Another clear advantage of WiMAX is its ability to provide nomadic connectivity. So far, WiMAX has not yet taken off in most developed countries, due to the already excellent coverage of Wi-Fi access points and cell phone towers. However, it still plays an important role in rural areas or underdeveloped countries, where it can also support extending the reach of fixed line connections.

Moving from one network to another should be seamless and transparent to mobile users. The running applications should preserve running sessions and implicitly IP addresses. The MobileIP protocol, which is an Internet Engineering Task Force (IETF) standard, offers an efficient, scalable mechanism for roaming within the Internet. Together with Wi-Fi and WiMAX, MobileIP can provide an “always connected” service independently of (but very similar to) proprietary third generation (3G) mobile networks.

Ubiquitous, transparent global roaming is an important issue in wireless telephony as well. UMTS, the Universal Mobile Telecommunication System, is part of the 3G cell phone technologies, a significant advance from 2G systems such as GSM. UMTS, using W-CDMA (Wideband Code Division Multiple Access), supports up to 14.0 Mbit/s data transfer rates in theory (with HSDPA – High Speed Download Packet Access). UMTS with HSDPA is part of the 3.5G or “beyond 3G” technologies. At the moment, users in deployed networks experience 3.6 Mbit/s download rates with HSDPA handsets.

The strong advantages of UMTS networks lie in their high degree of portability and interoperability. This makes it possible to have your mobile phone work anywhere in the world. UMTS phones (and data cards) are highly portable – they have been designed to roam easily into other UMTS networks, and network providers throughout the world have supported roaming agreements. In addition, almost all UMTS phones (except in Japan) are UMTS/GSM dual-mode devices, so if a UMTS phone travels outside UMTS coverage during a call, the call may be seamlessly handed off to available GSM coverage. Different countries support different UMTS frequency bands and networks must support a common frequency to work together. To enable a high degree of interoperability, UMTS phones usually support several different frequencies in addition to their GSM fallback.


\(^{68}\) http://www.wimaxforum.org/technology/
Using a cellular router, PCMCIA or USB card, customers are able to access 3G broadband services, regardless of their choice of computer (such as a tablet PC or a PDA). Using a phone that supports 3G and Bluetooth 2.0, multiple Bluetooth-capable laptops can be connected to the Internet. The phone acts as a router, but via Bluetooth rather than wireless networking (802.11) or a USB connection.

Most of the phones today support UMTS, but there are some that still do not because of the high battery consumption of UMTS. For example, with the exception of certain models, most BlackBerry smartphones are not currently 3G capable. Furthermore, Apple's iPhone does not support 3G and is restricted to using the EDGE standard. Apple claims that this is in order to maintain a reasonable battery life on the telephone. However, power usage of 3G is improving and Apple is rumoured to be releasing a 3G/UMTS iPhone in the second half of 2008.69

At the other end of the spectrum, we find low-power, short-range communications technology such as ZigBee, Bluetooth (version 3 of which is currently under development) and Wireless USB. The latter two use ultra wide band (UWB) spread-spectrum technology. UWB helps to increase data rates, robustness, security and energy consumption by using not a single frequency to transmit data, but “spreading” the signal across hundreds of frequencies and later re-assembling them at the recipient’s end.

Wireless USB is a short-range, high-bandwidth wireless radio communication protocol created by the Wireless USB Promoter Group. Wireless USB is based on the WiMedia Alliance’s Ultra-WideBand (UWB) common radio platform, which is capable of sending 480 Mbit/s at distances of up to 3 metres and 110 Mbit/s at up to 10 metres. The protocol was designed to operate in the 3.1 to 10.6 GHz frequency range and is used by many devices such as game controllers, printers, scanners, digital cameras, hard disks and flash drives.70

Bluetooth is a short-range wireless protocol used in creating wireless personal area networks (PANs). It facilitates both voice and data transmissions over short distances from fixed and/or mobile devices. It is supported by most modern mobile devices and computers, and can be used by mice or wireless keyboards. Bluetooth adapters and headsets can be acquired for very low prices (€2-20).

**Body area networks**

Body area networks (BANs)71 are an emerging communication paradigm that focuses on intra-body communication, i.e., wireless communication technology that links together devices on (or in close proximity to) the body, including implanted devices. Especially the latter is highly relevant in the context of novel health applications that rely on the permanent monitoring and logging of vital signs. BAN communication can, of course, be realised using traditional short-range wireless communication technology, such as ZigBee or Bluetooth, yet this approach would not be able to implicitly determine whether a device in range is really on the person’s body (or worn by the person) or if it belongs to another person in close proximity. Specific BAN technology such as NTT’s RedTacton72 uses the weak electric field of the body to transmit signals along the entire body surface, as well as to any device touched

69 For more on UTMS, see: http://en.wikipedia.org/wiki/UMTS#Interoperability_and_global_roaming
70 For more on Wireless USB, see: http://en.wikipedia.org/wiki/Wireless_USB
71 For more on Body Area Networks, see: http://www.ban.fraunhofer.de/index_e.html
72 http://www.redtacton.com
by the person (e.g., a door knob, a chair, a floormat). Others have proposed the use of vital parameters as a shared communication key between all on-body devices.\textsuperscript{73} In this manner, BANs offer better inherent confidentiality than traditional wireless communication. However, the ease with which BANs support the use of sensors on and inside the body might lead to a proliferation of biometric data use, e.g., for authentication and authorisation, for lifestyle applications or for health-related issues.

**Information dissemination**

Just as wired and wireless communication technology facilitate the increasing availability of digital data, information dissemination technology eases the spreading of such information – not just point-to-point but also among groups and in particular geographic regions. There has been an explosion of information dissemination platforms, from blogging and lifelogging websites, to P2P and mash-up networks, that allow users to easily post and share documents, images or videos.

Some of these applications are covered in related sections in chapter 3 of this document. In the following, we present just two relevant technologies: mobile web server and IP telephony.

**Mobile web server**

Since its proliferation as a device used to access the Internet, the mobile phone has only been used as client, i.e., for simple browsing or to access online services. However, the tremendous increase in the computational power of such devices, combined with the availability of high connectivity rates, raises the possibility of users having and maintaining their own personal, mobile web servers on their devices. Mobile web servers would allow users to easily disseminate information created with their mobile phones such as captured videos, images and audio streams as well as location information and environmental or vital sensory data.

The Mobile Web Server\textsuperscript{74} project at Nokia Research Center ported Apache HTTP\textsuperscript{75}, the most widely used web server in the world, to run on the S60/Symbian platform. Additionally, the project targets support for semi-automated web page generation, which significantly improves user experience. Unlike creating web pages and deploying a web server in the traditional Internet, which requires advanced technical skills or/and an administrator to carry on the job, now anybody can easily create and deploy web pages and share data from phones, even without any technical expertise.

**IP telephony**

There is a trend to move from traditional public switched telephony network (PSTN) systems to voice conversations sent over the Internet, also known as IP telephony. VoIP (Voice over IP) is an optimised protocol to transmit voice over the Internet. SIP, the Session Initiation Protocol, is a signalling protocol that is today widely used for setting up and tearing down multimedia communication sessions such as voice and video calls over the Internet.


\textsuperscript{74} For more on the Mobile Web Server, see: http://research.nokia.com/research/projects/mobile-web-server/

\textsuperscript{75} For more on the Apache HTTP server project, see: http://httpd.apache.org/
At the outset, IP telephony allows consumers to lower their communications costs, as VoIP accounts are often much cheaper than traditional fixed land lines (if not free). Also, IP telephony allows for free calls with other VoIP clients, charging only for routing back into the traditional PSTN.

A more significant advantage, however, is the ability of VoIP to make and receive calls as one would at home, anywhere in the world, at no extra cost – worldwide number portability. Phones like the NEC N900iL, many of the Nokia E-series phones, and several Wi-Fi enabled mobile phones have SIP clients hard-coded into their firmware, allowing them to operate independently of the mobile phone network. Many recent DECT portable phones support both traditional phone lines and several VoIP accounts in a single device.

With the migration from traditional telephony to these new kinds of services, many security questions regarding eavesdropping or wiretapping have been raised. For example, many consumer VoIP solutions do not support encryption yet. It is possible to use IPsec to secure P2P VoIP by using opportunistic encryption, but encryption and cryptographic authentication are not yet widely available at the consumer level. As a result, it is relatively easy to eavesdrop on VoIP calls (or even change their content) – an ability that before rested only with law enforcement authorities and the network operators. Now, however, an attacker with a simple packet sniffer running on a standard laptop can intercept VoIP calls over an unsecured connection. In fact, there are several open source solutions available that facilitate sniffing of VoIP conversations. In its recent study, Viper Lab warns that denial-of-service (DoS) attacks on VoIP networks will become an increasingly important issue. Attacks against service providers will escalate as unlicensed mobile access technology becomes more widely deployed. Viper Lab also says that “service providers are, for the first time, allowing subscribers to have direct access to mobile core networks over IP, making it easier to spoof identities and use illegal accounts to launch a variety of attacks”.

Undoubtedly, better security is desirable, but there are more things to consider. Even with mobile IP telephony, we hit the controversy between improving security, and thus protecting privacy in communications, on the one side, and the desire of law enforcement authorities to be able to monitor conversations, on the other. As the popularity of VoIP grows, and as users switch to VoIP in increasing numbers, governments are becoming more interested in regulating VoIP in a manner similar to public switched telephony network services. In the US, the Federal Communications Commission (FCC) now requires all interconnected VoIP service providers to comply with requirements comparable to those for traditional telecommunications service providers. VoIP operators in the US are required to enable law enforcement authorities to conduct surveillance pursuant to the Communications Assistance for Law Enforcement Act (CALEA).

Skype uses encryption for all data transmitted, which protects against eavesdropping but also impedes authorities from listening in to conversations, thus making Skype non-CALEA-compliant. The dispute on changing VoIP services to allow wiretapping is far from being resolved. Concerns about high costs of changing existing service infrastructures to be CALEA compliant and security holes that could be created as a result have been strongly raised.

---

Security expert Bruce Schneier, however, points out that identifying current conversation partners on Skype (to know who is talking to whom), for which technological solutions exist (such as embedding an undetectable signature in Skype packets\textsuperscript{78}), might be more relevant to law enforcement than the actual content of the conversation\textsuperscript{79}.

### Challenges

Among the main challenges arising from communication and dissemination technologies are these:

- How can we support the desire of people to engage in social discourse and disclose information about themselves, while ensuring that data are eventually forgotten or at least limited in diffusion?
- How can we ensure the safety of intimate communication systems, i.e., body area networks that carry highly sensitive medical data, both against eavesdropping and manipulation (control)?
- How can we strike a balance between communication privacy and the need of law enforcement to observe and inspect communication patterns of suspects in VoIP systems?
- How can we provide adequate security safeguards for wireless communication that is easy to use?

2.3 **New Architectures and Protocols**

The processing and exchange of information requires both architectures and protocols that enable different communication partners to collaborate. New technologies for (personal and industrial) information and application sharing pose challenges to privacy and trust, including specific threats from secondary data collection, content-based image retrieval, phishing, infiltration and widespread distribution of user-created content. This also includes the issue of linkability from image metadata, online reputation, online gossip, etc. Some technologies, such as digital identity standards, can be regarded as a possible response to increased data collection, by offering credential-based authorisation options (see also section 3.2.1 on cloud computing). This section attempts to describe some of the underlying architectures and protocols that facilitate such information sharing, in particular:

- database federations,
- the Internet of things and the EPC network,
- Web 2.0 and new methods and tools to create content on the Web, e.g., mash-ups.

Businesses and public authorities have long since begun to merge the plethora of databases they have created over the years, as well as the collections started by business partners or subsidiaries, into so-called database federations – virtual databases that offer a single comprehensive view of dispersed data sets. Database federations are particularly challenging due to their reliance on legacy applications as well as their stringent requirements on scalability. Advances in this area make it increasingly feasible to integrate previously fragmented information, thus potentially offering higher efficiency, better services and improved data integrity. However, the pooling of separate data sources complicate data access


controls, in turn requiring research into complex business intelligence applications that are able to honour the various disclosure policies associated with each individual data source. Researchers at IBM have coined the term “Hippocratic databases” to describe the feature of such systems in protecting personal data, especially in the area of health care.\textsuperscript{80}

Another approach to data integration comes in the form of EPCglobal’s “EPC network”, an architecture for sharing product information along the supply chain. Using RFID technology as a universal identifier on pallets, cartons and items, a unique EPC code enables the storage and retrieval of product-related data at each step of the supply chain. Sometimes described as the “Internet of things”, this architecture is envisioned to bridge the gap between the real world and the virtual world, offering a single point of entry to item-related data. In practice, the envisioned data exchange across company boundaries is complex, and free access of information is still the exception rather than the rule. However, the EPC network has the potential to significantly affect the storage and processing of consumer-level item data.

With the implementation of the EPC network still at a considerable distance, end-users are already experiencing another architectural revolution – on the Web. Since the early beginnings of static web pages, the architecture has since moved to a service-oriented approach, where information is not restricted to the format of a set of pages, but is dynamically generated as needed from a variety of sources. This asynchronous retrieval model, called “Ajax”, is the basis of today’s popular “mash-ups” – the fusion of multiple information sources into novel services. While Google popularised this, e.g., through its Google Maps service that lets users combine geographic information with high resolution maps, its rival Yahoo! has recently unveiled its “Pipes” architecture that aims at significantly simplifying this process, using, e.g., a simple graphical interface that allows even novices to merge and process online data.

JXTA is a set of open protocols and implementations that allows any connected device on the network, from cell phones and sensors to PCs and servers, to communicate and collaborate in a direct, peer-to-peer (P2P) manner.\textsuperscript{81} It was introduced by Sun Microsystems in April 2001 and is used by numerous members and big companies (e.g., by Nokia in its P2P server network, by Verizon in its “iobi” call management service\textsuperscript{82}). JXTA is used to create applications and services that enable people to collaborate on projects from anywhere using any connected device, to share computer services, such as processor cycles or storage systems, regardless of where the systems or the users are physically located, to create P2P networks, or to connect game systems.

Towards open mobile platforms

Departing from closed and difficult-to-program mobile environments such as Symbian, a recent trend in mobile systems is pushing towards open frameworks and programmer-friendly software development kits (SDK). The unveiling of the Google Android platform in November 2007 and the release of the Apple iPhone SDK in March 2008 aim to actively involve the developer community in creating mobile applications and, thus, improve the

\textsuperscript{81} JXTA: http://www.sun.com/software/jxta/
market adoption and penetration of mobile systems and devices.\textsuperscript{83} Android is a software platform and operating system for mobile devices based on the Linux operating system that has been developed by Google and the Open Handset Alliance.\textsuperscript{84} It allows developers to write managed code in a Java-like language that uses Google-developed Java libraries. Similarly, Apple’s iPhone SKD allows independent software developers to create and sell programs for the iPhone and iPod touch.

Several experts argue that mobile virtualisation solutions, similar to VMWare and Xen for desktop systems, are the future for guaranteeing mobile phone security. Virtualisation would also improve interoperability, enabling applications to be run on any mobile device, independent of its operating system. Big players such as T-Mobile, Motorola, Samsung, etc., are actively investing in the research and development of this virtualisation technology.\textsuperscript{85} However, no complete technical solution is available yet. Implementations are expected to come in several years. Gartner says that mobile device solutions won’t be ready until 2012.\textsuperscript{86} Even beyond that, adoption, user and corporate acceptance and efficiency remain uncertain.

**Challenges**

Despite the positive effects on business and economic potential resulting from opening mobile environments to third-party developers, the move also opens potential security vulnerabilities. Running only (or almost only) proprietary software, mobile phones are currently regarded as trusted, highly personal devices. But who will be responsible for user security in the future, if a third party application misbehaves or compromises the mobile device? This is of particular concern in the context of increasing malware threats for mobile devices. Will this significantly reduce the level of trust that users currently have in their mobile phones? Given that mobile phones store highly personal and sensitive data such as contact information, e-mail, confidential corporate documents and credit card and mobile payment applications, how can we ensure an appropriate level of data protection and application isolation? Many visions of a future smart environment rest on a personal trusted device that acts as a single trusted intermediary in unknown smart environments: what happens if these devices will be as prone to attacks as today’s desktop PCs and laptops?

Among the main challenges arising from new architectures and protocols are these:

- How can information be protected in global information flows across EPC networks and/or database federations?
- How will open mobile platforms change the perception of the mobile phone as a trusted device?
- Who owns information that has been passed through filters and aggregators multiple times?
- How will people manage their “online identity”?


\textsuperscript{84} Google Android: http://code.google.com/android/


2.4 **INFORMATION STORAGE AND PROCESSING**

Falling prices for digital storage media have led to a significant increase in data storage. Instead of having to minimise data collection due to the associated cost of storing it, today it is much cheaper to simply buy additional storage instead of having to perform a costly analysis of what to store. In this section, we present the state of the art in *storage components* such as memory and hard disks in terms of storing capabilities and price. The availability of cheap storage has already turned into a business model: Cloud computing services (see section 3.2.1) such as Amazon’s S3 offer redundant online storage for a few cents per gigabyte per month. This applies not only to companies and public institutions, but also to individuals and their private data: 1 terabyte of magnetic storage today retails for less than £100 on Amazon.uk (as of August 2008), allowing for the storage of hundreds of thousands of holiday pictures. This proliferation of storage not only affects data collection practices of public and private bodies, but also increases the risk to individuals who collect data that might cause embarrassment (to themselves if not to others), makes them vulnerable to criminal acts such as data or identity theft and could provide incriminating evidence against themselves in the context of criminal or civil investigations. With the availability of ever smaller storage devices that allow people to carry with them vast amounts of data, a considerable volume of which could be personal, there is also an increasing risk of loss or theft. In this section, we present technologies that enable individuals to collect huge amount of data, mainly audio and video streams, something that is today called *lifelogging*.

With the increase in data collection size, there is an equally growing need to make sense of stored data, to find relevant information and to distil *knowledge*. One avenue is to connect and combine multiple data sources through database federations, as outlined in section 2.3 (new architectures) above. At the same time, *data mining* algorithms based on statistical analyses are continually refined to extract statistical correlations between various parameters, or forecast developments. The US government MATRIX program, launched in the wake of the 11 September 2001 attacks, was on its way to becoming one of the most extensive data mining operations when it was officially discontinued.

**Magnetic storage**

The area of high-capacity data storage is currently dominated by magnetic and conventional optical storage.\(^88\) The traditional measure of technology progress is *areal bit density* (Gbit/in\(^2\)).

Conventional magnetic recording has been the leading technology for more than 50 years and has continually and significantly increased storage capacity. However, possible future advancements are limited by the physical properties of the medium. Storage disks are formed of microscopic magnetic grains, which in order to improve capacity, become so tiny that they lose their ability to hold their magnetic orientations at room temperature. Consequently, data on the disk are spontaneously erased.\(^89\) To overcome this limitation and significantly increase the areal density towards the terabyte hard disk, new technologies for magnetic storage such as *perpendicular recording* and *secondary actuators* have recently been introduced.

---

87 In August 2008, one could purchase an 8 GB memory stick on Amazon UK for less than £10 plus postage.

88 Optical storage uses laser light or electromagnetic waves near the light spectrum for reading and writing data. Examples of optical disc drives are CDs and DVDs.

While in conventional, longitudinal recording, the magnetic orientation of the data bits is aligned horizontally, parallel to the surface of the disk, perpendicular magnetic recording (PRM) orients data bits in a vertical fashion. In this orientation, smaller crystalline grains can be used that make it harder to reverse the magnetic orientation, resulting in smaller physical bits that are still stable at room temperature. The first PRM disks began shipping in 2006 and today represent the most dramatic introduction to significantly improved storage capacities. Hitachi's 1-TB 3.5-inch Deskstar 7K1000 (initially retailing at $400, was about half that in June 2008) is both the first terabyte drive in retail and Hitachi’s first 3.5-inch drive to use perpendicular recording. Estimates for the ultimate limit for a perpendicular recording system range from 500 Gb/in$^2$ to 1Tbit/in$^2$, the latter limit being reached in January 2007 by Fujitsu. However, new technologies such as heat-assisted magnetic recording (HAMR) and patterned magnetic media promise to overcome this limit.

By using a laser to heat a tiny spot on the recording medium, HAMR is expected to increase the limit of magnetic recording by more than a factor of 100 and produce storage capacities as great as 50 Tbit/in$^2$. Seagate believes it can produce 300 Tbit (37.5 Tbyte) hard disk drives using HAMR technology. In patterned media, the magnetic layer is created as an ordered array of highly uniform islands, each of which stores one single bit. Ideally, ordered nanohole patterned media enables future hard disk drive capacity potential to 1.2 Tbyte*1 for 2.5” HDD.

Holographic data storage

Conventional magnetic and optical storage systems rely on individual bits stored as distinct magnetic or optical changes on the surface of the recording medium. Holographic data storage overcomes this limitation by recording information throughout the volume of the medium and is capable of recording multiple images in the same area using light at different angles. Additionally, while magnetic and optical data storage records information one bit at a time in a linear fashion, holographic storage is capable of recording and reading millions of bits in parallel, enabling data transfer rates greater than those attained by optical storage. Holographic data storage drives are currently being sold by InPhase Technologies, which began shipping 300 GB disks in February 2007.

Millipede memory is a non-volatile computer memory stored on nanoscopic pits burned into the surface of a thin polymer layer, a good candidate to be used for micro drives. The technology was demonstrated by IBM Zurich at CeBIT 2005 and promised a data density of more than 1 Tbit/in$^2$. IBM planned to roll it into a commercial product by the end of 2007, but

---


95 For more on InPhase Technologies, see: [http://www.inphase-technologies.com](http://www.inphase-technologies.com)
today due to huge advances in other computer storage systems, like Flash\textsuperscript{96} and hard drives, the technology seems to have been abandoned.\textsuperscript{97}

Technologies presented at CeBIT 2008 showed improved storage capacities and a dramatic decrease in power consumption. Samsung announced the shipment of its newly developed 2.5-inch 500 GB hard disk drive for laptop computers for $300. 64 GB Flash SSDs were presented by both SanDisk and Samsung.\textsuperscript{98}

### Lifelogging systems

The term “lifecasting” describes the continual broadcast of events in a person's life through digital media. Typically, lifecasting is transmitted through the medium of the Internet and can involve wearable technology.\textsuperscript{99} The idea of lifecasting started in 1980 when Steve Mann started experimenting with wearable computing and streaming videos, but it was only 14 years later, with the boom of the Internet, that Mann started continuously transmitting his everyday life. Lifecasting has gained popularity and many other people have also been lifecasting their lives. Streaming of live video, capturing and publishing it on lifelogging websites has become a true social networking phenomenon.

Today, many sites such as Justin.tv, Ustream.tv and Camstreams offer free streaming services, making it possible for anyone with a computer, a webcam, a microphone and an Internet connection to continuously lifecast for free to a global audience and to archive the videos for a certain period of time or tagging footage to signal interesting and appealing videos. Streaming is often combined with wearable computing and GPS automatic location information and is favoured by technological improvements in audio and the invention of smaller, less intrusive cameras.

The SenseCam\textsuperscript{100} is a personal, wearable camera developed by Microsoft Research in Cambridge, UK, and is used as a lifelogging device in projects such as MyLifeBits\textsuperscript{101} (see below) and as a memory aid for Alzheimer patients. The camera takes images passively throughout the day, at several intervals, or triggered by potential chances in sensor measurements. Incorporated sensors include light-intensity and light-colour sensors, a passive infrared (body heat) detector, a temperature sensor and a multiple-axis accelerometer. Experiments with the incorporation of audio level detection, audio recording and GPS location sensing have also been conducted.\textsuperscript{102} Images are afterwards processed to detect events such as “shopping”, “driving”, “people present” and a lifelog calendar is created and possibly linked to relevant data found on the Internet. Cheap storage turns “lifecasting” into “lifelogging”, allowing not only for the dissemination of personal experiences but their permanent storage. The most prominent example of this is the “MyLifeBits” experiment by Microsoft researcher Gordon Bell, who has begun to capture most of his daily life in digital

\textsuperscript{97}For more on Millipede memory, see: http://en.wikipedia.org/wiki/IBM_Millipede
\textsuperscript{99}For more on Lifecasting (video stream), see: http://en.wikipedia.org/wiki/Lifecasting_(video_stream)
\textsuperscript{100}For an Introduction to SenseCam, see: http://research.microsoft.com/sender/projects/sensecam/
\textsuperscript{101}For more on the MyLifeBits Project, see: http://research.microsoft.com/barc/MediaPresence/MyLifeBits.aspx
form, using the SenseCam to capture his interactions during the day, GPS to record his movements and e-mail to track his online activities. The project addresses both challenges in lifetime storage, and software research for data processing. MyLifeBits aims to make annotation easy, including text annotation on right click, voice annotation and web browser integration. It includes tools to record web pages, IM transcripts, radio and television and leverages an SQL server to support hyperlinks, annotations, reports, saved queries, pivoting, clustering and fast search. Further features such as document similarity ranking and classification are also explored.

**Information processing and data mining**

Similar in nature to Microsoft’s SenseCam, but with a much larger scope, is the “reality mining” project at the Massachusetts Institute of Technology (MIT). The idea is to develop data mining algorithms that process information gathered by sensors, such as security cameras, wearable devices or simply cell phones, to understand and predict human behaviour.

MIT researchers have already conducted a number of interesting reality mining experiments. By measuring the variability of a salesman’s tone of voice at a British call centre and how much he listened versus how much he spoke, scientists could predict with 89 per cent accuracy whether the customer was going to buy. By analysing data collected by “sociometers” worn by employees of a German bank – badge-like devices that hang from subjects’ neck and record movements, tone of voice and location – they could tell whether people felt overworked, who was happy or who felt their group was well-managed. Furthermore, they could automatically learn personality traits in any group. Similar studies can be conducted on a large scale using data gathered by mobile phones to determine how productive and how happy people are. Other possible applications include detecting SARS (Severe Acute Respiratory Syndrome) and predicting crime.\(^{103}\) Researchers at Nokia Research and the University of California, Berkeley, have used movement patterns from mobile phones travelling in cars to predict traffic patterns with a much higher accuracy than purpose-built roadside traffic sensors.\(^{104}\)

Data mining has long since played an important role in law enforcement, especially after the 11 September 2001 attacks. The Multistate Anti-Terrorism Information Exchange Program\(^{105}\) (MATRIX) was a federally funded data mining system originally developed for the Florida Department of Law Enforcement to help identify terrorists. While the program supposedly worked well, it was shut down in June 2005 after federal funding was cut in the wake of public concerns over privacy and state surveillance.\(^{106}\) The system analysed government and commercial databases to find associations between suspects or to discover locations of completely new “suspects”. The database and technologies used in the system were housed by Seisint, a Florida-based company since acquired by LexisNexis.

MATRIX used the Factual Analysis Criminal Threat Solution (FACTS) application, which is a technological, investigative tool allowing query-based searches of available state and public


\(^{104}\) See [http://lagrange.ce.berkeley.edu/media/media-coverage.html](http://lagrange.ce.berkeley.edu/media/media-coverage.html)


records in data reference repositories. The data reference repository for the FACTS application contains public records from thousands of locations (i.e., county courthouses and other public records locations) of US individuals and businesses. Such data include FAA pilot licences and aircraft ownership, property ownership, federal terrorist watch lists, etc., but exclude telephone calling logs or records, mailing lists, bank account numbers or account balances, airline reservations or travel records.

Aggregating information from several databases is not a trivial process. Data come in different forms, which make relating them to other forms of digital data challenging. Few technologies allow automatic conversion of different kinds of raw data collected by sophisticated sensors in a format that permits the data to be mined effectively. Information gleaned from such processes is by definition probabilistic in nature.

**Challenges**

Among the main challenges arising from new architecture and protocols are these:

- Do people own their own data? How can we ensure that they do?
- How can we balance the benefits of technologies such as reality mining and tracking applications with the privacy problems they raise?
- How will personal mobile storage affect personal data theft and corresponding crimes (e.g., fraud, blackmailing)? How can we effectively protect personal mobile data from third party access, even if the data are lost?
- How will lifelogging affect interpersonal relations?
3 CHALLENGES FROM SOCIO-ECONOMIC DEVELOPMENTS

Commerce and economic growth thrive on creating products and services that people want. To sell products and services, companies need to get as close to the consumer as possible, to understand what he or she wants or needs (even if the consumer does not yet realise what it is he or she wants or needs), to stimulate the consumer’s interest in new products or services, to be reasonably sure that the consumer will be able to pay (eventually) for the new product or service, to have a clear idea of what appeals to the consumer and what doesn’t, and so on. Hence, to improve their customer relationship, companies want data about the consumer, so that they can personalise their products and services as much as possible. It is, of course, best if companies get that personal data directly from the consumer-citizen with his or her consent. Sometimes, inducements are useful ways to get that data. Thus, for example, supermarkets offer loyalty cards with which their customers can get a “reward”, usually a small discount on their grocery bill. To get a loyalty card, the customer has to provide some personal data which the supermarket chain may share with other allied companies. In other instances, the customer may, in effect, be forced to provide personal data if he or she wants to get the product or service. For example, if someone wants a mortgage, the bank or financial institution will want to know a lot about him, his financial situation, where he works, what his salary is, his ability to repay, his employment history, what credit cards he holds, whether he has any serious medical condition that may prevent his being able to make the payments, whether he has a criminal record and so on. Similarly, if he wants some home or life or medical insurance, he will need to provide a lot of personal data. In other cases, if a customer buys an appliance, he may be encouraged to provide some personal data in order to “register” the product with the supplier, to get an extended warranty or after-sales service or to be able to download software a second time in the event that his computer crashes. In still other cases, if the individual wants a job, whether in the public or private sector, he will need to fill in an application form that requires a lot of personal data, where he lives, how old he is, his educational and previous employment history, his medical condition, whether he has ever been found guilty of any offences and so on. These are just a few of the many ways to get personal data.

After having supplied all these personal data, however, the curious customer may have some questions. Who “owns” the data? Who will have access to those data? How will the data be used? How will they be secured and protected? Will the data be passed on to third parties? Will the customer have an opportunity to see what is recorded about him and to correct that information if it’s wrong?

These and other questions are also being asked about new and emerging socio-economic applications arising from the increasing ubiquity of information technologies. This chapter reviews some of the most important new applications and, in particular, examines the challenges they pose to privacy and trust.

---

108 In Germany, banks often receive this information from a credit-rating agency (SCHUFA) which also receives customer-related information from banks. SCHUFA has been criticised heavily for its scoring practices, for example, you may not be rated as creditworthy if you live in the wrong neighbourhood even if no negative information is available about you personally.
3.1 PRIVACY-CHALLENGING BUSINESS FUNCTIONS

3.1.1 Personalised advertising

Personalised or behavioural advertising involves the tracking of a consumer’s activities online – including the searches the consumer has conducted, the web pages visited and the content viewed – in order to deliver advertising targeted to the individual consumer’s interests. In an ambient intelligence environment, the consumer will be tracked in space and time, and may find advertising directed at him wherever he goes and whatever he does, as vividly shown in the Steven Spielberg film Minority Report where Tom Cruise races through corridors lined with adverts specially targeted at him (with delicious irony, they urge him to “get away from it all”).

It is virtually impossible for consumers to escape from being bombarded non-stop by advertising. Taxis and buses now carry adverts, metro stations are lined with advertising, TV programming is constantly interrupted with someone trying to sell us something, the cinema insists on hitting its captive audience with 15 minutes or so of adverts before showing the feature film. Even the clothes we wear and the accessories we carry often display someone’s logo, so that we become walking adverts. But these are all relatively static forms of advertising. Advertising in the 21st century is much more dynamic, personalised and targeted, not at groups, but at individuals. The individual sitting in front of his computer or using his mobile phone is now subjected to one-on-one advertising and what he sees increasingly is based on some clever algorithm that has interpreted his apparent behaviour and interests.

Amazon and its emulators have been demonstrating this algorithmic approach for some years. “Based on your previous searches, we think you’d be interested in…”

Day by day, search engines such as Google and Yahoo are cornering the advertising market because they have been very good in tracking the user’s search interests. They already store a user’s Internet address along with the searches made and websites visited from that address. That IP address is super valuable to the likes of Google. If someone has your IP address, it makes it much easier to gather the additional information needed to identify you. Google records the IP address associated with every search it handles. It comes as no surprise that Google insists that an IP address should not be regarded as personal data. As The New York Times points out, there may be more than one person who uses a computer, just as there is often more than one person who uses a home telephone, but few people would say that this means phone numbers aren’t personal. The companies involved say customers’ privacy is protected because no personally identifying details are released.

So with that IP address, companies such as Google keep log files recording every search term used and page displayed on the user’s screen. Adverts in Google’s e-mail services are placed there based on keywords found in the user’s e-mail. According to one survey in the UK, 40

110 In the UK, the press attracted 40 per cent of £19.4 billion spent on all advertising in 2007. TV captured 24 per cent, while the Internet as the third largest medium accounted for nearly 16 per cent. The Internet was the fastest-growing medium for advertising in 2007, up 39.5 per cent, while the press fell 1.6 per cent and TV grew by 2.3 per cent. Advertising Association, The Advertising Statistics Yearbook 2008, Press release, 9 June 2008. http://www.adassoc.org.uk/index.html
per cent of free e-mail users are unaware that their e-mails are being scanned for keywords used to target them with “personalised” advertising.\textsuperscript{112} By monitoring every click and keystroke users make online, service providers can generate more revenue from advertisers who have a better idea of the consumer’s interests as deduced from what the consumer has been searching for and looking at online in the past few hours or days. Some have likened the monitoring of our online activity to eavesdropping. Some say the next big growth in advertising will emerge from efforts to offer ads based not on the content of a web page, but on knowing who is looking at it. That, of course, means gathering more information about consumers.\textsuperscript{113}

“Cookies”, bits of software deposited on the surfer’s computer when he visits a website, have been used for many years to track the surfer’s repeat visits to the website and which web pages he looks at on a given site. Now it is possible to generate profiles of users by monitoring their IP traffic at Internet service providers. Since the use of cookies began, advertisers and service providers have become much more ingenious in milking all the data they collect from users. As an example, the social networking website MySpace has sold the merits of it HyperTargeting ad program to more than 50 large advertisers, including Ford and Taco Bell. The service scours user profiles for interests and then delivers related ads. Facebook also has a new advertising system based on data from its members’ profiles.\textsuperscript{114} Meanwhile, Yahoo has announced plans to trial Google AdSense for Search service, which will deliver relevant Google ads alongside Yahoo’s search results.\textsuperscript{115}

“Web analytics” is the buzzword used to describe the study or analysis of tracking users as they navigate through an individual website and on the Web itself. Software analyses how users relate to the content, and whether it is working effectively to connect users and adverts by collecting real-time information on Internet behaviour, including how users got to a particular site and where they went afterward, how long they visited a site and which content resulted in interest or interaction.\textsuperscript{116}

\begin{quote}
\textbf{eMarketer estimates that US spending for behaviourally targeted online advertising will reach $775 million in 2008, but projects that it will reach $4.4 billion by the end of 2012. Behavioural targeting is getting increasing attention from advertisers, publishers, the public, politicians and mainstream media. For now, though, it contributes little to total US Internet ad spending – only 3 per cent is projected for 2008. “The growth of behaviourally targeted online advertising has been delayed by incomplete development of technology, brand marketers that prefer to have their ads appear with relevant content and concerns over violating consumer privacy,” says David Hallerman, senior analyst at eMarketer and author of the report, \textit{Behavioral Targeting: Marketing Trends}.\textsuperscript{117}
\end{quote}

\begin{flushleft}
\end{flushleft}
Advertising and discriminatory pricing

As an example of what can happen when users are tracked, their viewing analysed and then targeted with “personalised” adverts, consider the case of Alaska Airlines. The airline has introduced a system to create unique adverts for people as they surf the Web. The company combines data from several sources to paint a picture of the consumer, as he clicks past the airline’s adverts. Then, as each web page loads, an advert is swiftly assembled with an offer designed especially for each individual consumer.\textsuperscript{118}

To select adverts for each Web surfer, Alaska Airlines gathers data such as the person’s geographic location, the number of times the person has seen an Alaska Airlines advert and whether the person visited the company’s website. Other considerations are the person’s purchase history with the airline and his or her experience with lost bags, delays and flight cancellations.

The company feeds data about which people click on its adverts to a company called Proclivity Systems, which analyses how price-sensitive customers seem to be. Then, in an instant, one customer gets an offer for a flight from Seattle to Portland for $99 and another is quoted $109.

A Boston company, DesignBlox, assembles the airline’s adverts. The system works like that Yahoo introduced in 2007 which instantly creates custom adverts based on retail data about which products are selling and which ones are not. Yahoo says that the percentage of people who click on these adverts is two to three times the percentage who click on more static adverts.

Another data practice at Alaska Airlines is called retargeting, which involves recording who visits the website, and then turning those data over to the airline’s advert delivery company, Atlas, a unit of Microsoft. Next, when those people are elsewhere on the Web, Atlas shows them an advert. That means that people who have visited Alaska Airlines’ site receive adverts that are different from those seen by people who have not.

Deep packet inspection

The precision of new advertising practices are based in part on new monitoring techniques, known as “deep packet inspection”, which enables a more in-depth view of what the surfer is up to, of every web page visited, every e-mail sent and every search term entered. Instead of basing their adverts on the content of a web page, advertisers now seek to base their adverts on knowing who is looking at the web page (e.g., dog owners will see adverts for dog food even if they visit a website dealing with personality disorders).

Deep packet inspection is, as its name suggests, a form of inspecting, filtering or examining computer network packets, the data they carry and/or the header part of a packet. The packet can be inspected for viruses, spam, tampering, denial-of-service attacks or other criteria to decide if the packet passes inspection and can be sent on to its destination or if it needs to be routed to a different destination. Deep packet inspection can be used in support of different functions or applications including security, data mining, eavesdropping, censorship, anti-

piracy – and targeted advertising. Deep packet inspection (DPI) devices have the ability to look at Layer 2 through Layer 7 of the OSI model. This includes headers and data protocol structures as well as the actual message. A packet can be redirected, tagged, blocked or reported to some other agent in the network. DPI allows service providers to “readily know the packets of information you are receiving online—from e-mail, to websites, to sharing of music, video and software downloads”. With deep packet inspection, Internet service providers can monitor all of their customers’ activity on the Web and thereby gain a lot of information about their interests and habits.

Phorm uses deep packet inspection to inspect what requests a user makes to a website and what content comes back from the website. Phorm redirects the user’s traffic to a device that inspects the traffic, adds a Phorm cookie (if it’s not already there) and then sends the packet on to its original destination. Phorm scans each visited webpage for the frequency of key words as a representation of what the web page was all about. The user is identified by a random number not by his IP address. By understanding the types of websites visited, Phorm provides a service that enables advertisers to target their adverts at particular users.

The increasingly sophisticated approach to individualised or personalised or behavioural advertising has generated many concerns as reflected in the media, the comments made by privacy advocates and public opinion. In one typical survey, almost three-quarters of those surveyed by TNS Global on behalf of TRUSTe, the consumer privacy organisation, said that they are aware that their browsing history may be collected for advertising purposes. Almost all indicated that they would like to have more say in how their information is used. Behavioural advertising has also aroused the attention of regulators. The US Federal Trade Commission issued guidelines (proposed principles) for behavioural advertising in December 2007, but some say they don’t adequately deal with the new technologies and new advertising practices. They say that consumers are targeted without their consent and that too little is known about the protection of the harvested personal information.

### FTC’s proposed principles re behavioural advertising

The FTC is encouraging industry to adopt and implement its principles regarding behavioural advertising, which are as follows:

1. **Transparency and consumer control**

---

120 This paragraph paraphrases an article on DPI in Wikipedia. http://en.wikipedia.org/wiki/Deep_packet_inspection#cite_note-Chester2006-4
124 FTC commissioner Jon Leibowitz has been quoted as saying, “People should have dominion over their computers. The current ‘don’t ask, don’t tell’ in online tracking and profiling has to end.” See Story, Louise, 5 Nov 2007, op. cit.
Every website where data is collected for behavioral advertising should provide a clear, concise, consumer-friendly and prominent statement that (1) data about consumers’ activities online is being collected at the site for use in providing advertising about products and services tailored to individual consumers’ interests, and (2) consumers can choose whether or not to have their information collected for such purpose. The website should also provide consumers with a clear, easy-to-use, and accessible method for exercising this option.

2. Reasonable security, and limited data retention, for consumer data

Any company that collects and/or stores consumer data for behavioural advertising should provide reasonable security for those data. Consistent with the data security laws and the FTC’s data security enforcement actions, such protections should be based on the sensitivity of the data, the nature of a company’s business operations, the types of risks a company faces, and the reasonable protections available to a company.

Companies should retain data only as long as is necessary to fulfil a legitimate business or law enforcement need. FTC staff commends recent efforts by some industry members to reduce the time period for which they are retaining data. However, FTC staff seeks comment on whether companies can and should reduce their retention periods further.

3. Affirmative express consent for material changes to existing privacy promises

A company must keep any promises that it makes with respect to how it will handle or protect consumer data, even if it decides to change its policies at a later date. Therefore, before a company can use data in a manner materially different from promises the company made when it collected the data, it should obtain affirmative express consent from affected consumers. This principle would apply in a corporate merger situation to the extent that the merger creates material changes in the way the companies collect, use and share data.

FTC’s proposed principles re behavioural advertising (continued)

4. Affirmative express consent to (or prohibition against) using sensitive data for behavioural advertising

Companies should only collect sensitive data for behavioural advertising if they obtain affirmative express consent from the consumer to receive such advertising. FTC staff seeks specific input on (1) what classes of information should be considered sensitive, and (2) whether using sensitive data for behavioural targeting should not be permitted, rather than subject to consumer choice.

5. Call for additional information: Using tracking data for purposes other than behavioural advertising

FTC staff seeks additional information about the potential uses of tracking data beyond behavioural advertising and, in particular: (1) which secondary uses raise concerns, (2) whether companies are in fact using data for these secondary purposes, (3) whether the concerns about secondary uses are limited to the use of personally identifiable data or also extend to non-personally identifiable data, and (4) whether secondary uses, if they occur, merit some form of heightened protection.
Nevertheless, advocates of deep-packet inspection see it as a boon for all involved. Advertisers can better target their pitches. Consumers see more relevant adverts. Service providers who hand over consumer data share the advertising revenues. And websites can make more money from online advertising, a rapidly growing, multi-billion dollar industry.

Among the companies that have developed behavioural advertising techniques are Front Porch and NebuAd in the US and Phorm in the UK. They are selling their monitoring services to Internet service providers who are finding new ways to generate additional revenue streams from the user activity that they already monitor. Front Porch, NebuAd and Phorm work by installing devices on the networks of the Internet service providers with whom they have agreements. The devices monitor all of the web pages each user visits and the terms he or she searches for. The ISPs then build a profile that associates the surfer’s computer with those web pages and search terms. The profile is based on a unique ID allocated at random to each Internet user which is held only on the user’s computer and by Phorm or its counterparts. Then, as the user surfs, the adverts he sees on various websites are based on his profile.

Phorm has reached agreement with three of the largest Internet service providers in the UK, BT, Virgin Media and Carphone Warehouse, which together account for about 70 per cent of the UK broadband market. The Phorm service is called Open Internet Exchange (OIX). Some say that by offering targeted advertising, ISPs and publishers can charge up to 100 times as much as they would earn from traditional advertising based on content.

One of the key issues raised by behavioural advertising is whether the individual Internet user has to opt out or is given the choice of opting in. Phorm and the others say that consumers can opt out of the monitoring (if they know where to look in their customer service agreements). Some ISPs have altered their customer service agreements to permit the monitoring.

Consumers have not complained to any great extent about data collection online because, say privacy experts, the collection is largely invisible and unknown to them. The largest Web companies say that privacy fears are misplaced, and that they have policies in place to protect consumers’ names and other personal information from advertisers. Moreover, they say, the data are a boon to consumers, because the adverts they see are more relevant to their interests.

Phorm says that it protect consumers’ personal data by assigning a number to each consumer rather than their IP address so that no one (except them, of course) can identify individual consumers. The company also says visits to some sensitive sites are not tracked. Phorm sugarcoats its proposed service by offering a free service to consumers called Webwise, which it...

---

128 Brodie, Sophie, “ISPs go for targeted online ads service”, The Telegraph, 15 Feb 2008. http://www.telegraph.co.uk/money/main.jhtml?view=DETAILS&grid=&xml=/money/2008/02/15/cnphorm115.xml. The story also quotes Kent Ertruglur, chairman and chief executive of Phorm, as saying, “Less than 10 per cent of Internet pages are monetised from an advertising perspective. Showing ads based on who’s looking at a page rather than the content will expand advertising to the long tail of pages beneath the home page.”
claims will reduce the number of irrelevant adverts and protect against malicious content or phishing attacks by warning consumers when they are browsing fraudulent websites.\footnote{Brodie, op. cit.; Edgecliffe-Johnson, op. cit.}

**Interception of communications**

BT and perhaps by association Phorm got themselves into some hot water over a “technical” but secret trial conducted by BT. Some 18,000 BT customers were subjected to Phorm’s ad-serving technology between September and October 2006 and “tens of thousands” more customers in the summer of 2007.\footnote{The Guardian said it had learned that BT and Phorm tested the service in secret in the summer of 2007. See Arthur, Charles, “Phorm fires privacy row for ISPs”, The Guardian, 6 Mar 2008. http://www.guardian.co.uk/technology/2008/mar/06/internet.privacy. The Register carried a story in which it cited Phorm as saying that the 2007 tests involved tens of thousands of BT customers. See Williams, Chris, “BT’s ‘illegal’ 2007 Phorm trial profiled tens of thousands”, The Register, 14 Apr 2008. http://www.theregister.co.uk/2008/04/14/bt_phorm_2007/}

BT customers were not made aware of the tests, nor of the fact that their web traffic was being intercepted.\footnote{Tests conducted by Internet companies using NebuAd were also carried out without consumers’ prior, explicit consent. Nakashima, Ellen, “NebuAd Halts Plans For Web Tracking”, Washington Post, 4 Sept 2008. http://www.washingtonpost.com/wp-dyn/content/article/2008/09/03/AR2008090303566.html} BT has admitted that “All users were unaware they were participants in the trial.” Cambridge University professor Richard Clayton has opined that, as customers’ personal traffic data were intercepted, processed and used for personalised adverts without anyone’s consent, BT appears to have committed a criminal offence under the UK’s Regulation of Investigatory Powers Act 2000 and that BT should be prosecuted accordingly. Prof Clayton has claimed that BT also contravened the Data Protection Act by processing the data, which he regards as personal data, without the customers’ consent. BT has insisted that no personal data were processed, stored or disclosed during this trial.\footnote{Espiner, Tom, “BT Phorm trial leak rekindles row”, ZDNet.co.uk, 6 Jun 2008. http://news.zdnet.co.uk/communications/0,1000000085,39430496,00.htm. See also Waters, Darren, “BT advert trials were ‘illegal’”, BBC News, 1 April 2008. http://news.bbc.co.uk/1/hi/technology/7325451.stm. The Article 29 Data Protection Working Party said in April 2008 that it “preferred” that search engines not collect and use personal data to serve personalised adverts unless the user had consented and signed up to the service. Waters, Darren, “Search engines warned over data”, BBC News, 7 April 2008. http://news.bbc.co.uk/1/hi/technology/7335359.stm}

**Private sector initiatives**

Phorm had Ernst & Young and 80/20 Thinking Ltd assess its system’s privacy features.\footnote{Edgecliffe-Johnson, Andrew, “Phorm leaps as big internet service providers sign on”, Financial Times, 15 Feb 2008. The FT story said Ernst & Young and Privacy International assessed Phorm’s privacy features, while Phorm says on its website that “its privacy claims have been validated under best industry practices, both through an independent audit conducted by Ernst & Young and a Privacy Impact Assessment undertaken by Simon Davies, managing director of 80/20 Thinking and Director of Privacy International.” http://www.phorm.com/about/launch_agreement.php. The privacy impact assessment was conducted by 80/20, not Privacy International.} This was a good move by Phorm. Not only does it have the benefit of (somewhat) undercutting possible opposition to a new service, but also it has genuine value for companies when they develop a new product or service to which they suspect there may be some opposition. This “preview-review” by reputable, independent third-party organisations (especially a privacy advocacy organisation) will help the company in seeing whether they have any “chinks in their armour”, any aspect that they have not addressed. If the company
genuinely believes in the efficacy of their product or service, such a review by independent third parties will help them determine whether there are any privacy-enhancing improvements that could be made to their product before releasing it to the public. It also helps the company to build bridges with those from whom it might face the most vociferous opposition. Such strategies have value for the company in potentially increasing consumer trust and confidence in a new offering because it has been reviewed by an independent third party whom the consumer is more likely to trust than the company.

In the US, AT&T and Verizon, two of the nation's leading Internet service providers, pledged in September 2008 to refrain from tracking customer Web behaviour unless they receive explicit permission to do so. According to a report in The Washington Post, the announcement “represents a challenge to the rest of the Web world”. How many companies will follow in their wake remains to be seen.

**Regulatory requirements**

Following discussions with Phorm, the UK Information Commissioner’s Office (ICO) put out a statement on 4 April 2008, which it then revised, putting out a much longer version on 8 April, in which it said that even if Phorm does not process personal data, it will still need to comply with the Privacy and Electronic Communications Regulations 2003 (PECR). Regulation 6 of the PECR says that a user must be informed when a cookie is placed on his computer, given clear and comprehensive information about the purpose of the storage and given the ability to refuse its being placed on his computer.

Regulation 7 requires the ISP to get the consent of users to the use of their traffic data for any value-added services. “This strongly supports the view that Phorm products will have to operate on an opt in basis to use traffic data as part of the process of returning relevant targeted marketing to internet users,” said ICO.

ICO also said that, based on the explanation given by Phorm, “there does not appear to be any detriment to users in the operation of the Phorm system as those who choose to be involved will only have the information used to match them against an advertising category and then present them with targeted advertising while browsing the internet. The ISP does not create lasting records of browsing habits in this context and do not seek to link living individuals to that information as it profiled and sent to Phorm. It also appears that users who opt out do not have their web browsing habits profiled.”

On the allegations that Phorm’s service or that of the ISPs with which it has an agreement is an interception of communication under the terms of the UK Regulation of Investigatory Powers Act 2000 (RIPA), ICO deferred to the Home Office, which is responsible for compliance with RIPA. The Home Office has yet to comment on the issue.

In July 2008, EC Information Society Commissioner Viviane Reding wrote to the UK government asking that it clarify the legality of Phorm’s system. In September 2008, the Department for Business, Enterprise and Regulatory Reform (BERR) responded that it was

---


satisfied that the system complied with EU regulatory requirements, but said deployment must be done with consent and make it easy for people to opt out. The fact that profiles are based on a unique but random number rather than the users’ IP address coupled with the fact that Phorm does not keep a record of actual sites visits were cited as reasons for its legality. BERR said Phorm should be operated on the following basis:

- The user profiling occurs with the knowledge and agreement of the customer.
- The profile is based on a unique ID allocated at random which means that there is no need to know the identity of the individual users.
- Phorm does not keep a record of the actual sites visited.
- Search terms used by the user and the advertising categories exclude certain sensitive terms and have been widely drawn so as not to reveal the identity of the user.
- Phorm does not have nor want information that would enable it to link a user ID and profile to a living individual.
- Users will be presented with an unavoidable statement about the product and asked to exercise a choice about whether to be involved.
- Users will be able to easily access information on how to change their mind at any point and are free to opt in or out of the scheme.

Needless to say, Phorm was pleased with this outcome. The European Commission does not seem satisfied with the way in which the UK government has dealt with Phorm. In February 2009, a spokesman for Commissioner Reding said that “The Commission may have to proceed to formal action if the UK authorities do not provide a satisfactory response to the Commission's concerns on the implementation of European law in the context of the Phorm case.”

**Media attention**

The sustained coverage by the news media, especially influential newspapers such as *The New York Times* and *Washington Post* in the US and their counterparts in Europe, such as *The Guardian*, *The Financial Times* and *El Pais*, have made an impact. In June 2008, the fourth biggest cable operator in the US announced that it was not going to continue with deep-packet inspection.

Charter Communications had been planning to harvest the stream of data from each Internet customer for clues to their interests and then make money from advertisers who would use the information to target online pitches. Charter officials said the data-collection effort would have protected personal information, but critics likened the practice to wiretapping.

Rep. Edward J. Markey (D-Mass.), chairman of the House Energy and Commerce subcommittee on telecommunications and the Internet, said “They made the right decision in halting their test.”

---


Other Internet companies also suspended or cancelled trials of NebuAd’s deep-packet inspection technology. In early September 2008, NebuAd announced that it was suspending its plans to deploy the technology while Congress reviews privacy concerns associated with it. The company also announced the resignation of its founder and chief executive Bob Dykes. While NebuAd has had a hard time in the US, Phorm in the UK appears to be succeeding, perhaps it has adopted a more open public relations strategy. Its shares jumped about 20 per cent in early September 2008 after it announced that BT, Carphone Warehouse and Virgin Media were still onboard for major trials of its technology and that it had found interest with other ISPs in the UK and abroad.

The political use of behavioural advertising

Behavioural advertising, in its various forms, is used not just for selling products or services by companies. A recent story in the Washington Post shows how politicians are using the same tactics as companies to target prospective voters and supporters.

Web users monitored more closely every day

A recent analysis, conducted for The New York Times by the research firm comScore, shows that large Web companies are collecting more data than ever before about what people search for and do on the Internet. These companies use that information to predict what content and adverts people most likely want to see. They can charge steep prices for carefully tailored adverts because of their high response rates. Increasingly, advertisers place their adverts according to how much sites know about Web surfers.

Previously, Web companies could only monitor the actions of consumers on their own sites, but over the last couple of years, the Internet giants now can follow people’s activities on far more sites.

ComScore estimated how many times major Web companies collect data about their users in a given month. It analysed 15 major media companies’ potential to collect online data in December 2007. The analysis captured how many searches, display ads, videos and page views occurred on those sites and estimated the number of adverts shown in their ad networks. These actions represented “data transmission events” – times when consumer data were zapped back to the Web companies’ servers. Five large Web operations – Yahoo, Google, Microsoft, AOL and MySpace – recorded at least 336 billion transmission events in the month.

Yahoo came out with the most data collection points in a month – about 110 billion collections, or 811 for the average user. MySpace and AOL were not far behind. Traditional media companies, however, came in far behind. For example, Condé Nast, which publishes

---

Vogue and The New Yorker, had only 34 data collection events for the average site visitor in the month. The New York Times Company had 45 and the Walt Disney Company, 64.  

The News Corporation is exploring ways to use information that MySpace members post on that site to select adverts for those members when they visit other News Corporation sites.

**Throwing grit in the wheels of capitalism**

If you viewed privacy-enhancing technologies as a spectrum or a continuum, out there to the far left would be programs such as Adblock, a bit of software put together by a lone individual that literally blocks ads from appearing on your computer screen. To corporatists who line their pockets with the revenues they generate by targeting adverts, such software is downright seditious, and its purveyor is throwing grit in the wheels of capitalism itself. To top it off, the blacklisting software is free.

EasyList and the Adblock Plus software with which it works may be the most popular and most effective of all the ad-blocking systems on the Web, according to The Washington Post.144 Using EasyList, which is also free, Adblock Plus screens out not just pop-ups, but virtually every other Internet ad form, including in-page display and video. They are the brainchildren of Rick752, as he is known online, who created the ad-blocking software in his spare time and who otherwise is a machinist in upper New York state.

**Challenges**

Behavioural advertising raises a number of privacy challenges:

- Are consumers adequately informed that (when) their online behaviour is being monitored?
- Do consumers have to opt out of such services or should they rather have the choice of opting in?
- How visible should monitoring companies make opt-in or opt-out information? Should notices to the consumer be “unavoidable”?145
- How well do the monitoring companies protect consumer data?
- What would constitute informed consent (opt-in) to participate in such services?
- If several members of a family use the same computer, is there a risk that younger members will be hit with offensive or inappropriate adverts based on the browsing habits of the adult user?
- Should the monitoring companies be required to make certain consumer disclosures in regard to this practice and, if so, what? For example, how the data are collected, used and protected?
- Should certain standards be set for monitoring consumer online behaviour?
- Should industry be encouraged (required) to self-regulate such practices? Or should the practice be subject to regulatory oversight?
- Are consumers favourably disposed towards seeing adverts that are more generally applicable to their interests or are they more generally opposed to their being monitored?

---

• Are the actions of the companies engaged in behavioural advertising adequately monitored and especially with regard to how they use and reuse the data they have collected?

3.1.2 Electronic payment systems

The increasing use of electronic payments system goes beyond traditional credit-based payments using credit or debit cards. While both types of payment systems have long since enabled the detailed tracking of consumer spending, developments such as RFID-based credit cards and micro payments, which are described in section 2.1.2 mobile payment, will make use of non-cash payments, especially for small amounts, easier and thus leave more digital traces. Gartner Research, for example, forecasts rapid growth in the use of those, especially in the field of “digital money” like the Linden dollar in Second Life.146 All of this creates more possibilities to track consumers’ behaviour and creates a new set of problems, which have not been considered until now.

According to old and new research results, the biggest concern of users of every electronic payment system in both worlds, off- or online, is the fear of fraud and misuse of their data by a third party such as cyber criminals. The growing volume of this kind of cyber crime seems to confirm this.147 While the methods of cyber criminals to gain personal data or misuse payment systems have become very sophisticated in recent years, the prevention and even the definition of cyber crimes has not advanced to the same extent, as the European Commission stated in 2007.148 At the same time, these issues have shed light on a broad variety of existing and possible problems. All stakeholders, not only consumers, are affected in multiple ways. For example, on the one hand, enterprises are interested in gaining more knowledge about and improving offers for individual customers by collecting more data about individual spending and payment behaviour. On the other hand, they are also interested in increasing the use of business-to-consumer (B2C) commerce with micropayments or credit cards, which require high security standards and trust by consumers in companies’ reliability. The spread of virtual or “online” money raises issues too. Unlike real money, there is no system of protection and trust for customers as the case of the virtual Ginko bank in Second Life showed in 2007 (a run on the bank forced its closure).149

Challenges

As a consequence of all these different dimensions and problems, the further development of electronic payment systems suggests many different scenarios in the field of collecting, storing or processing data, which are direct or indirect challenges to privacy and trust, which can be divided into three broad categories:

1. challenges by cyber criminals:

• Low security barriers as well as complicated and user-unfriendly systems for electronic payment systems open the way for cyber crime through the collection of payment data by means of phishing, hijacking or other methods of social hacking.
• The storage of customers’ data including payment data by companies is often poorly protected by inadequate security systems, which creates an opportunity for malefactors to break into company databases.

2. challenges by function creep:
• exchange or sales of payment data between companies,
• misuse of data for consumer scoring,

3. challenges by virtual money:
• lack of control and regulations for the distribution and use of online money, which leads to misuse, fraud, cyber crimes, etc.,
• regulations about convertibility and stability of such money.

While the first challenge is present in all areas including media, legislation and business, the other challenges are neglected. Challenges arising from electronic currencies were discussed in the early and mid-1990s but never became relevant due to the failure of early attempts to establish electronic currencies. In general, there are two distinct types of digital cash: identified digital cash and anonymous digital cash. Identified digital cash contains information revealing the identity of the person who originally withdrew the money from the bank and allows the money to be tracked as it moves through the economy. Only anonymous electronic currencies, which work just like real paper cash, do not challenge citizens’ privacy. A standardised, regulated and well-spread system for anonymous digital payments would be the best possible response.

3.1.3 Supply chain management

Business and supply chain management (SCM) has long recognised the value of advanced monitoring technology. “You can only manage what you can measure” is an old business adage. Recent technology such as RFID has already seen widespread deployment, and providers of enterprise resource planning (ERP) software are actively working on integrating a wide range of sensors that can offer real-time business analysis value. While mostly about business processes, such deployments can nevertheless raise privacy and trust issues. One example is the use of location-tracking systems within the fleet management of a company that allows employees to use cars for private purposes. In these cases, companies may track and analyse the movement of employees during working hours as well as in their private time. A balance needs to be struck between the privacy rights of employees and the claim of companies’ business interests.

Most of the current debate about supply chain management has focused on item-level tagging with RFID technology for providing after-sales services. From a privacy point of view, this is the most problematic aspect of SCM since the end-user is then in possession of the product. If the identification, positioning and tracking technologies (see section 2.1.1) are used to collect data not only during the production and distribution processes, but also in sales to consumers, this would transform the after-sales services and, as a consequence, the actual use of products, especially if the consumer is not given the possibility to opt in to additional services.

Possible implications could be that companies deny a guarantee when consumers deactivate the identification technology or if a tracking function reveals an unintended use of the product. Other possibilities are tracking, recording and analysing general patterns such as the position of the object, the frequency and intensity of its use, etc. Also considered to be harmful is the illicit readout of RFID tags by third parties. While the use of RFID in after-sales has already been the subject of recent research\textsuperscript{151}, there are some aspects of SCM and especially after-sales that have been less covered until now. One of these white spots is the use of customer relationship management (CRM) applications. CRM has mostly been considered as a tool for intra-industry relationship management, but now companies are using it to address consumers as well.\textsuperscript{152} The deployment and use of such applications are not in themselves problematic, but in combination with item-level tagging, electronic payment systems, etc., modern CRM is able to build a realistic picture of each customer from the collected information.

**Challenges**

The use of RFID in the ways described above creates a series of challenges to privacy and trust in relation to:
- the secondary use of information for behavioural marketing (see section 3.1.1),
- the sale of data to scoring companies,
- the misuse of data, for example, when hackers gain access to inadequately protected databases.

### 3.1.4 Location-based services

Location-based services are one of the possible new business functions that arise from the public availability of location tracking technologies, which has to meet three criteria for this purpose: (1) define the position with high accuracy, (2) transmit the current location to a service provider and (3) do so in real time.\textsuperscript{153}

While the challenges of using this technology for commercial applications such as fleet management are already the subject of discussions (see section 3.1.3), the consequences for private users are often underestimated.\textsuperscript{154} The most popular ideas for services in this category are “friend/child finders”, location-based advertising and travel guides. There are two possible points of departure for these services. The first is receive-only position determination systems such as GPS while the other is remote positioning systems using triangulation (as cell phones do). With receive-only systems like GPS, the user theoretically makes a conscious decision to enable a transmitter to transmit his position, while other systems may be transmitting the

user’s position without his knowledge or such transmissions are required for the regular use of the device. Due to the variety and increasing diffusion of devices such as mobile transmitters, RFID or Wi-Fi systems, position-determination with remote systems seems somewhat less subject to user control. As a consequence of the growing popularity of such systems, the number of possible services seems nearly unlimited. With the convergence of location-based services and other novel technologies and services such as personalised marketing (see section 3.1.1) or after-sales services (see section 3.1.3) such as those featuring RFID chips, experts see significant challenges to citizens’ privacy as well as to society as a whole.

**Challenges**

Since most of the applications rely on a combination of technologies and business functions that have already been analysed with regard to their privacy implications, here we discuss causes and responses. Apart from legal responses, most experts see a big problem in the consumers’ lack of awareness of the impact of the technology’s use. Positioning systems have become very popular while most users are not aware that the systems not only provide information, but also are able to send information and receive responses such as adverts. In view of “consumer malaise,” “soft” instruments such as awareness-rising campaigns and education may be more efficient than formal regulatory or legislative responses.

Location-based services are still in their infancy, yet they promise to significantly affect citizens’ privacy through their potentially comprehensive location records assembled in the process of service provision. While service contracts providing navigation or location-based points-of-interest listings might still be managed by traditional purpose-bound approaches, peer-to-peer exchanges between friends and family members might affect an individual’s privacy to a much greater extent. Without the help of powerful user interfaces (e.g., privacy-enhancing technologies), individuals will not be able to properly negotiate their “privacy boundaries” in dynamic everyday settings.

### 3.1.5 Digital rights management and intellectual property rights

Digital rights management (DRM) technologies are used to protect intellectual property rights. Because digital information such as text, images, sounds and other content can be freely copied, DRMs have been introduced to enforce predefined limits on the possible distribution and use of protected work. Imposed policies can be fine-grained, for example, in limiting the number of times protected information can be viewed, allowing only selective access to certain parts of the protected information, enforcing time windows during which certain access privileges are available or tracking who has received the protected information, what, when, how many times they read it and for how long. Online verification and authentication systems are a common building block of DRM, which opens up avenues for detailed tracking of consumer activity. Furthermore, the Sony DRM episode has proven the


157 Long, Murray, op. cit.
potential of creating security vulnerabilities in systems where DRMs are used, and hence compromising personal security.\textsuperscript{158}

Digital rights technologies have stirred vigorous discussions about who has rights over what information for what purpose. The status quo will not survive unchanged.\textsuperscript{159}

Trusted computing and DRM are two very active and closely related areas of industry development of importance to cyber trust. DRM refers to approaches by which owners of digital content (information, software, music, films, games, etc.) can control the copying and distribution of their content to protect their copyright, and be paid for its use. This is technically very hard to do in any general way, especially when the content is used on general-purpose computing devices such as PCs. Trusted computing provides low-cost hardware integrated into common computers and other information appliances to improve the security achievable.

In essence, a “trusted platform” is authenticated – you know that it is what you think it is, and that a digital image on it is what you think it is. It typically uses specialised hardware to overcome the security problems caused by the essential modifiability of software.

Early versions now available allow secrets such as cryptographic keys and sensitive documents to be held in protected storage, for a co-operating chain of software to securely record what programs are loaded into the computer, and for secure transmission of that record to another computer. Controversially, the protected storage areas may include information secured against the user of the computer – for example, copyrighted material where the copyright owner allows access to the content only through approved software.

Controlling what runs on which platform does not in itself tell you anything more about the reliability of the digital image, or the reliability of the combined system, or the interactions between the digitised material and the system, or any of the other sources of insecurity or lack of dependability. However, in a situation where there is an overall system management environment which governs what should be running on the platform, trusted platforms can make a big contribution to security. They also support the enforcement of software licensing. For both these reasons, the computing industry has devoted a lot of attention to establishing standards for trusted computing platforms. The issues arising from the adoption of this technology revolve around who makes the decision about what should and should not be running on the platform – by definition, the technology is only useful under conditions of strong system management.\textsuperscript{160}

Some have criticised the “classic DRM” approach for destroying the consumer’s trust in the market due to the prophylactic suspicion of every consumer.\textsuperscript{161} They suggest other business

\textsuperscript{161} Bizer, Johann, Rüdiger Grimm and Andreas Will, “Privacy4DRM: Nutzer- und datenschutzfreundliches Digital Rights Management”, \textit{DuD - Datenschutz und Datensicherheit}, Vol. 30, No. 2, 2006, pp. 69-73. For the complete study, see Grimm, Rüdiger, Stefan Puchta, Michael Müller et al., “Privacy4DRM:
models, which they call “user-oriented DRM”. They propose the usage of pseudonymity concepts and award of seals of approval regarding data protection to restore the consumer’s trust in the market.

Bizer et al. made an empirical analysis of privacy concerns related to the use of different DRM technologies from which they concluded that vendors collect more personal data than needed for selling their wares. They describe three ways to protect digital rights: “strong DRM”, “fair use DRM” and DRM with commission schemes. They recommend that vendors put more trust in consumers and provide more transparency regarding the use of personal data in the context of DRM.

Copyright and IPR

Today we see increasing use of technological copyright mechanisms – including information systems architectures – which may have impacts on the privacy and related interests of users of information products.162

Downloading copyrighted material such as songs and films has, of course, been an issue for some years. Lately, in an effort to curtail the practice, some law-makers have adopted a “three strikes and you’re out” approach (after repeated warnings, the user is barred from the Internet). Internet service providers have also been criticised in allowing users to download such material too.

As the music industry struggles against the practice of perceived illegal downloading of copyrighted material, a recent study from the University of Washington suggests that media industry trade groups are using flawed tactics in their investigations of users who violate copyrights on peer-to-peer file sharing networks.163 The study found “a serious flaw” in how trade groups identify alleged file-sharers. It suggests that some people might be improperly accused of sharing copyrighted content, and could even be purposely framed by other users. The researchers concluded that enforcement agencies are looking only at IP addresses of participants on peer-to-peer networks, and not what files are actually downloaded or uploaded. The researchers demonstrated a way to manipulate IP addresses so that another user appears responsible for the file-sharing. In their paper, the researchers argue for greater transparency and public review of intellectual property enforcement actions.

http://www.bmbf.de/pub/privacy4drm_studie.pdf

http://folk.uio.no/lee/publications/technologisation_copyright_eipr_final.pdf

As part of his analysis, Lee Bygrave focuses on the applicability to this issue of the European Directive on copyright of 2001, the US Digital Millennium Copyright Act of 1998 and the EC Data Protection Directive.

ISPs are fighting back against charges saying that they contravene fundamental rights. To ensure their property and exploitation rights, the music and film industries began using DRM techniques in recent years, but their approach was criticised by most experts for destroying the consumer’s trust in the market due to the prophylactic suspicion of every consumer. Some critics said the term Digital Rights Enforcement (DRE) would be more a more accurate descriptor. In addition to the inherent distrust of users, DRM systems pose serious challenges to consumer privacy. In a study, funded by the German Ministry of Education and Research, Bizer et al. made an empirical analysis of privacy concerns related to the use of different DRM technologies. In their “Privacy4DRM” study, they identified several challenges to privacy from DRM systems, principally because the systems aim not only at securing rights, they also collect and store personal data so that the industry can see who is doing what and, based on this information, can initiate possible law enforcement actions.

In addition to the bad press and consumer reactions to DRM technologies, the uncontrolled collection and storage of consumer data has enabled DRM-embedding companies and third parties to use the data for consumer profiling. As a result of their analysis, Bizer et al. defined a set of legal requirements for DRM systems, for example, that DRMs should only be allowed to collect specified data, which are only allowed to be used for specified purposes and not to be processed any further than necessary for the specified purposes. They also formulated a transparent way to do this and proposed the usage of pseudonymity concepts and the award of seals of approval regarding data protection to help restore the consumer’s trust in DRM or DRM-embedded products.

**Challenges**

Core challenges remain:

- How can or should content creators, producers and suppliers be rewarded for their work in the face of widespread downloading by a high percentage of Web users?
- How should the transparency of DRMs be improved, so that users know when they are being used and what personal information the DRMs may be capturing and transmitting back to the content providers?
- Are regulation and standardisation needed to govern the use of DRMs?

### 3.2 NOVEL BUSINESSES AND BUSINESS MODELS

In the following pages are examples of new businesses and business models that raise privacy issues. This section is not comprehensive by any means but the examples used indicate how new technologies and applications not only generate new business opportunities, but also

---


have implications for the protection of personal data that must be scrutinised carefully if these new opportunities are going to be successful, in the eyes of consumers, the media and policymakers and other stakeholders.

3.2.1 Cloud computing

Information is increasingly stored and processed by third parties on behalf of both companies and individuals, i.e., address books, calendars, messages, documents and other elements are kept in Web-enabled locations to be accessible from anywhere, at any time, by any means of communication. This is not entirely different from, say, hosting a company website, but while so far this has been a rather fragmented business run by countless larger and smaller “hosting” companies, recent years have seen an unprecedented concentration of this process, as companies such as Google and Amazon have started to “rent out” their custom-built, large-scale hardware and software infrastructure to both individuals and companies.

This move has been dubbed “cloud computing”, in order to illustrate the fact that both data storage and processing has moved from a single server to a worldwide cluster of distributed machines, i.e., the “cloud”. The main novelty of cloud computing is the massive scalability that it can achieve, its main feature, the focus on selling services, rather than simply renting out hardware such as servers. A similar development, though with a more industrial focus, is expressed in the terms “software as a service” (SaaS) and “platform as a service” (PaaS), as offered by companies such as Salesforce.com (with their Force.com service) or Bungee Labs (BungeeConnect).

In comparison to grid computing and data centres, the main difference lies in the level of manual set-up and administration necessary: cloud computing, SaaS and PaaS offer standardised services that can be used with minimal set-up and maintenance, thus significantly lowering the cost of entry for users, both in time and money.

Amazon was one of the first companies to allow customers access to its infrastructure as part of its “Elastic Compute Cloud” (EC2) offering. In early April 2008, Google announced a limited test of its new Google App Engine, an online development environment for building and running Web applications on the same hardware that Google uses to run its search services. Xcerion’s “icloud” offers users a virtual “Cloud OS” that runs various desktop applications (e.g., presentation software, calendar, e-mail), similar to the Google App offering. In recent years, Microsoft has tried to create a comparable cloud of its own. It is investing heavily in infrastructure and has built data centres around the world. Microsoft CEO Steve Ballmer said it will launch “Windows Cloud” (perhaps with a different name) in November 2008. He said “new business models” would accompany its introduction: “Some things will be sold, some things will be put out on a subscription basis, some things will be monetised through advertising. We need to make sure there’s a model and a platform that supports all of that.”

---

Cloud computing further blurs the boundaries between traditional data storage and processing models. Especially in the end-user domain (in contrast to industrial applications running on SaaS/PaaS infrastructures), this might drive the centralised storage and processing of a large amount of personal information, especially if free use of the “cloud” is conditional upon allowing the cloud operator some sort of access (e.g., in aggregated format or to insert an advertisement) to this information.

Google, best known for its search engine, was the first company to build a huge computing cloud – a nexus of hardware, software, data and people providing online services. In Google’s vast data centres, the computing equivalents of power stations, hundreds of thousands of machines are cleverly linked to act as one. Google collects vast amounts of data from its users and from the Web. And it has hired an army of bright engineers to devise new services that make use of these resources.\(^\text{169}\)

Most importantly, Google has figured out a way to make money from its cloud. By giving away its services, the firm creates plenty of space for targeted advertising, mostly in the form of small text-boxes related to users’ search queries. These are auctioned, and buyers pay only if users click on their advertisements. Google has thus created a virtuous cycle. As the largest search engine, Google attracts more advertisers and can serve up more relevant advertisements. This in turn attracts more users and advertisers, and so on. This mechanism is well known from Gmail and poses the same challenges to privacy criticised by experts.\(^\text{170}\)

**Challenges**

The preceding examples point to two things: first, the concept of cloud computing is a somewhat loose concept and, second, it will lead to challenges to the privacy of consumers, no matter what model finally prevails.

3.2.2 Internet Protocol Television (IPTV) and convergence of electronic media

IPTV (Internet Protocol Television) is the most recent development within the broad field of digitalisation and convergence of television, telephones and the Internet.\(^\text{171}\) The so-called *triple play* (see section 2.4) is one major argument to enforce the build-up of new network infrastructures and to provide every household with broadband access.\(^\text{172}\) But unlike the convergence of, for example, telephony with the Internet (VoIP), IPTV marks a fundamental change, with technological requirements such as high speed networks, a new IP addressing system and much more broadband infrastructure.\(^\text{173}\) Behind all these technological considerations, which dominate current discussions in industry and among regulators, the IPTV convergence and digitalisation creates a challenge to privacy, affecting all stakeholders, policy-makers, businesses and consumers.

Challenges

While the use of telephony was never anonymous because of its one-to-one characteristic, television broadcasting is anonymous as it is a one-to-many transmission, where it is generally not possible to track who receives a broadcast and what is received. But if television is now distributed via the Internet, viewers can be identified because IP addresses can be resolved. So it becomes possible to monitor who (at least which IP number) watched what, for how long and how often. This loss of anonymity creates socio-economic as well as socio-political challenges.

- One possible consequence is that the recorded data can be used to create user profiles. This could be used for personalised advertising according to what individual consumers like to watch.
- Another threat is that these data can be combined with other data, for example, from credit or consumer cards, which will contribute to the transparent consumer. Further examples of secondary uses, which are mentioned elsewhere in this report, as well as misuse by third parties can be envisaged.

The socio-political impacts have not yet been considered in any depth until now, even though there may be harms to our fundamental rights. Hanne Sophie Greve, a former judge at the European Court of Human Rights, has commented that the possibilities of tracking and analysing consumers and their consumption patterns could harm the right of free media use. It could have an impact on how people use media and it increases the possibilities for influencing or manipulating public opinion. Some experts conclude that it is necessary to extend the regulations on the confidentiality of telecommunications to cover our use of media. Do we really want others to know which media we consume, how often and for how long?

3.2.3 E-energy and smart metering

E-energy promises to revolutionise the use of and control over energy by using ICT technologies. The roots of it lie in the European energy market liberalisation of 1999, the 2000 renewable energy law in Germany (which forced energy providers to buy renewable energy produced by private households) and the 2002 European Energy Exchange. The spectrum of possible elements of e-energy is broad and differs with every study on this topic. For instance, a study for the German government on the potential of ICT as an enabler for energy efficiency covers several areas such as network management, data networks, measuring technologies, etc.
The core element in the vision of e-energy, however, that relates to privacy and trust of consumers is measuring technologies, especially the installation of a “smart meter” in private households. Enabled and enforced through the continuing advances in ICT and the current debate surrounding renewable energy, sustainability and rising energy prices, the use of smart home automation systems and novel user interfaces and applications should help to reduce private energy consumption. Once installed, smart meters can observe and control in real-time the energy consumption of domestic electrical devices, especially if these have an interface for communicating their current and future energy needs from the meter. Direct contact with online energy markets allows the smart meter then to collaboratively schedule optimal operation times of appliances such as freezers, fridges or washing machines or to order electric energy as needed, based on current prices and availability (see, for example, the SESAM project\(^ {177}\) or the digitalSTROM initiative\(^ {178}\)). It can also communicate current and future consumption information to the home owner and propose or encourage energy savings, or send this information to energy providers in order to allow them to better forecast future demand and to avoid overcapacities. Finally, detailed demand and network load information is needed for stable control of so-called virtual power which is formed by a multitude of small decentralised generators including photovoltaics, wind power and combined heat and power plants.\(^ {179}\)

![Figure 3: Possible smart metering data flow](image)


In fact, smart meters close the information gap for understanding energy use pattern and to implement more efficient control mechanisms in general. The figure above shows the possible data flow enabled by the wide diffusion of smart meters that could also enable the provision on new energy services.

\(^{177}\) \[http://www.uni-flensburg.de/sesam/\]
\(^{178}\) \[http://www.digitalstrom.org/\]
The EU directive on end-use energy efficiency and energy services calls for the installation of individual meters and major European energy providers have already started pilot projects or initial deployments, including the following:

- **United Kingdom**: A consortium is planning an automated meter reading (AMR) pilot project with approximately 1,000 household customers. The project aims at reading existing meters optically and transmitting the data over TV cable or satellite links. Over TV cable, the power supplier receives metering data while customers receive information about tariffs, which are displayed on the TV set. If only a satellite link is available, metering data are transmitted over GPRS or another packet switched network.

- **Italy**: Over a five-year period beginning in 2000 and ending in 2005, Enel invested €5 billion for deploying smart meters to its entire customer base (30 million), motivated by cost savings for administration, reduction of electricity theft and stabilisation of the grid by reducing peak load during summer time. Enel is offering its customers a multitude of different tariffs. Meters were developed together with IBM and include a PLC modem for transmitting data to a so-called concentrator, which acts as the interface to existing IP networks. Most meters are read via a GSM link because this network has the broadest coverage.

- **Netherlands**: The Dutch ministry of economic affairs decided in February 2006 to replace all electricity and gas meters by AMR systems. For the implementation, a project group was installed which analyses the main advantages of AMR systems and defines the main functionalities.

- **Germany**: Recently, the German energy provider EnBW announced an AMR pilot with 1,000 homes. Energy consumption will be monitored and transmitted every 15 minutes.

- **Canada**: The Ontario Energy Board in Canada has been active in trying to define the technology and develop the regulatory framework for implementation of smart metering. Smart meters were to be installed in 800,000 homes by 2007, with an eventual goal of 100 per cent penetration by 2010.

The DigitalSTROM and Adhoco initiatives work towards integrating e-energy logic directly into future devices and household appliances. DigitalSTROM uses a chip attached to each device which enables wired communication between the sensor and the Web server, both of which are responsible for accounting and control. In contrast, Adhoco is based on a wireless approach. It uses ZigBee to link sensors and devices to the central base station, which also contains a self-learning mechanism to minimise energy consumption and to further personalise settings such as temperature and light.

---


184 [http://www.heise.de/newsticker/Pilotprojekt-mit-vernetzten-Stromzaehlern--/meldung/88561](http://www.heise.de/newsticker/Pilotprojekt-mit-vernetzten-Stromzaehlern--/meldung/88561)
Challenges

In addition to the advantages, smart metering (or in a broader sense, e-energy) creates some serious challenges to the consumer’s privacy and trust. The aforementioned report to the German ministry of economy stated these privacy threats quite clearly: “Theoretisch wäre es denkbar, dass durch die systematische Auswertung von Verbrauchsdaten gezielt Nutzungsprofile einzelner Haushalte erstellt und zu Marketingzwecke verwendet werden könnten. Das Verbrauchsverhalten der Kunden könnte dadurch auch für Dritte in hohem Maße transparent werden und u.U. zu Mißbrauch führen.”

This means it could disclose information about inhabitants’ activities. Data mining algorithms might be capable not only of inferring the consumer’s current and past activities from such data, but also of detecting habits and particular events (e.g., when others come to visit). An important system design parameter, therefore, is the level of granularity at which local energy measurements are stored and/or transmitted to the utility provider. This leads directly to the question which actor is allowed to collect, analyse and aggregate energy consumption data in a system that is – at least in Germany – still dominated by a few quasi-monopolists.

Because consumers cannot avoid using electricity in modern homes, challenges in this domain need to be met by clear legal regulation to prevent misuse or secondary use of data gathered by such technologies.

3.2.4 E-health

In days gone by, most people could assume that their medical records were a matter between them and their doctors. Such, however, is no longer the case, if indeed it ever was. Paper-based medical records are being superseded by electronic health records (EHR).

Many people have access to our health records

Many more people can, and do, have access to our electronic health records than most people might think. Robert Gellman wrote a rather humorous article about an encounter with a friend (Fred) who was wondering whether he should accede to a request to participate in some medical research in view of his concerns about keeping private some of his medical data. Gellman explained who might already have access Fred’s records. The list was long, starting, presumably, with everyone in his physician's office. “If Fred was also treated in a hospital, dozens or even hundreds of hospital workers might have had access to his records. This includes physicians, residents, nurses, ward clerks, orderlies, nutritionists, physical therapists, pharmacists, billing clerks, administrators, and others… Fred has other providers who know about his condition. A pharmacist, laboratory, or x-ray facility may know. These providers, like his doctor and hospital, have staff, lawyers, accountants, and others who see patient records. … Information flows from providers through clearinghouses to insurers, health plans,

185 Franz, Oliver, Matthias Wissner, Franz Büllingen et al., “Potenziale der Informations- und Kommunikations-Technologien zur Optimierung der Energieversorgung und des Energieverbrauchs (eEnergy)”. Studie für das Bundesministerium für Wirtschaft und Technologie, WIK-Consult; Fraunhofer-Verbund Energie, Bad Honnef, 2006, p. 38.

186 The Standing Committee of European Doctors (CPME) defines electronic health record as “a comprehensive medical record or similar documentation of the past and present physical and mental state of health of an individual and the medical procedures done in electronic form and providing for ready availability of these data for medical purposes”. http://www.cpme.eu. The Art 29 Data Protection Working Party adopted the same definition in its Working Document referenced below.
and HMOs. All of these organizations have staff, outside lawyers, accountants, computer service companies, and government regulators. Any of those individuals might have access to Fred’s information. So might his employer, who paid for his insurance. If the employer’s personnel department processed his claim, then people there already knew something about his condition. Even if they didn’t process the claim, the employer might ask the insurer to disclose information for a review of health care costs. Workers’ compensation claims involve additional institutions…” And on it goes. Gellman says his best guess is that somewhere between 1,000 and 10,000 individuals might have access to Fred’s records.

The UK is in the process of implementing a £12.7 billion information technology scheme which would involve a national database with the electronic health records of all citizens. The project has been described as the biggest non-military IT development in the world. It is envisaged that tens of thousands of NHS staff with security clearance would have access to millions of patients’ files – numbers that make Gellman’s estimates seem rather conservative. Is it any wonder, then, that doctors have reservations about a centralised government database of health records? A survey by The Guardian found that nearly two-thirds of family doctors said they intended to boycott the government’s scheme to put the medical records of 50 million National Health Service (NHS) patients on a national database. It found 59 per cent of GPs were unwilling to upload any record without the patient’s specific consent and were increasingly concerned about the government’s plan to automatically upload the records of everyone who does not register an objection. According to The Guardian story, government ministers said unless someone objected, it would be assumed that they had given “implied consent”.

The UK programme to modernise the NHS’s information technology systems is in line with European initiatives. In June 2006, the European Commission adopted a new strategy to promote the transformation of European healthcare, as part of the Commission’s i2010 policy framework. The ultimate goal is to enable access to the patient’s electronic health record and emergency data from any place in Europe. The Commission’s initiative was sparked in part because of the rising costs of medical care and the increasing chunk it takes out of the economy. The Commission’s e-health action plan regards the development of interoperable healthcare systems across the Union by 2010 as a priority. The Commission estimates that, by 2010, e-health spending may account for up to five per cent of the total

---

187 An HMO, Health Maintenance Organization, is a specific type of health care plan found in the United States.
191 This “implied consent” is at variance with the Art 29 WP document referenced below wherein it says patients must give their explicit informed consent and that opt-out solutions do not meet the requirement of explicit consent.
health budget of the 25 Member States from just one per cent in 2000 (for 15 Member States).  

In July 2008, the European Commission launched two initiatives to improve the safety and quality of care to people who require medical assistance while travelling or living abroad: a Recommendation on cross-border interoperability of electronic health record (EHR) systems and the Smart Open Services (SOS) project. The Recommendation aims to provide Member States with basic principles and guidelines for ensuring that doctors can gain access to vital information on patients whom they are trying to treat, wherever such information may be located in Europe. The SOS project, co-funded by the European Commission, is supported by 12 Member States and their industry players, to demonstrate the benefits of such interoperability. It will enable health professionals to access specific medical data such as current medications of patients from other EU countries, which, said the Commission, could save many patients’ lives in emergencies.

Gaining trust

One of the biggest challenges in implementing e-health concepts is gaining the public’s confidence that their electronic health records will be safe and secure. According to the British Medical Association, quoted in The Guardian story, “The government will not regain the confidence of the public or the profession unless it can demonstrate that its systems are safe.” The UK government appears to have an uphill struggle to win the hearts and minds of the family doctors, let alone the public, three-quarters of whom said in the aforementioned survey that they thought medical records would become less secure, and half thought the records would be vulnerable to hackers and unauthorised access by officials outside the NHS.

The public’s concerns are justified. Protecting medical privacy is more difficult today than just a few years ago for many reasons:

• More patient information is collected, both in volume and in types of information.
• More people have access to patient information, including medical caregivers, researchers, and administrators in the health care system and, in many cases, employers and government agencies outside it.
• Patient information is more easily accessible because it is increasingly stored in digital form (and so it can be transmitted more easily than in paper form).
• Patient information is held for very long periods of time, and the longer it remains in existence, the greater the opportunities for abuse.
• More patient information is being collected by types and in volumes that are intended to aid medical practitioners in predicting future medical conditions with greater accuracy.
• Patient information (such as DNA information) is being (or soon will be) collected that has relevance to individuals related to the patient (parents, siblings, current and future offspring), thus raising the potential for significant violations of medical privacy and complicating both the technical and ethical issues involved in managing such information.

194 http://www.ehealthnews.eu/content/view/210/59/
196 Waldo, James, Herbert S. Lin and Lynette I. Millett, Engaging Privacy and Information Technology in a Digital Age, Computer Science and Telecommunications Board, National Academies Press, Washington, DC,
Repurposing medical records

In the US, collected medical records provide a storehouse of information that can be used in a variety of ways other than those intended when the information was first collected. Such records can also be used for the marketing of particular drugs or for the denial of medical health insurance coverage. The health care domain has many stakeholders, some engaged in business, others in treatment and research, and it is often difficult to draw clear distinctions between where information is gathered for one purpose and is used for another.\(^{197}\)

With the availability of electronic health records, the temptation to use the collected data in multiple ways in addition to the original purpose is strong. It is helpful, though difficult, to distinguish between the practice, science, business and regulation of medicine.\(^{198}\)

The lines between proper and improper use of health information are unclear. For example, public health authorities may want to know of an infected person’s sexual contacts when they are trying to contain a sexually transmitted disease.\(^{199}\) In the US, an insurance company disputed patient claims for costs and wanted to see the patient’s messages on Facebook, MySpace and many other online sources. In a court dispute, the judge agreed with the insurance company.\(^{200}\)

Is regulation effective?

Waldo et al. say there are basically four approaches to address the challenges posed by electronic health records, namely, industry self-regulation, legislation and regulation, consumer/patient awareness, and official advocacy.\(^{201}\)

Somewhat moot is how effective each of these approaches is. In the first three years after the US Health Insurance Portability and Accountability Act (HIPAA) regulations came into force, thousands of complaints alleging violations resulted in just two criminal prosecutions, no civil fines and many agreements to fix problems that may have occurred without any penalty.\(^{202}\) In the long run, an enforcement regime of some sort is likely to be needed to ensure substantial compliance with the regulations, but that may not be enough. Waldo et al. say an institutional advocate for medical privacy in the US government, or in state governments, would help to


\(^{198}\) Waldo, p. 213.

\(^{199}\) Waldo, p. 228.

\(^{200}\) Waldo, p. 229.

\(^{201}\) Waldo, p. 216. See also Rothstein, Mark A., “Keeping your genes private”, *Scientific American*, Sept 2008, p. 43, wherein it is said that of 36,000 complaints, only one civil monetary penalty was assessed in the five years since April 2003.

ensure that adequate attention to privacy is paid in policy-making that might have an effect on privacy.\textsuperscript{203}

Determining the proper balance between access to information and protection of privacy in the business, practice and science aspects of medicine under the new realities of medical treatment is not something that can or should be done casually or by some small group either inside or outside the industry. The decisions made in this area will have an impact on the lives of everyone, and will affect the cost, efficacy and range of treatments. Greater clarity regarding the trade-offs between individual privacy and the use of this information would allow more informed discussion of alternatives for decision-making.

**A new risk scenario**

The Article 29 Working Party has said that “EHR systems pose significant challenges in ensuring that only appropriate health professionals gain access to information for legitimate purposes related to the care of the data subject… an EHR system must be considered as a new risk scenario for the protection of sensitive personal data” and, as such, calls for additional and possibly new safeguards.

In Europe, patient data are governed in part by the Data Protection and e-Privacy Directives. The Electronic Commerce Directive\textsuperscript{204} also applies to the provision of online health services. The latter Directive, principally by virtue of its internal market clause, contributes to the legal certainty and clarity needed for the provision of online Information Society services throughout the Union. The European Commission recognises the importance of the confidentiality and protection of patient data if e-health is to be successful. Its e-health action plan says, “Further steps might be considered if they could show that even greater legal certainty would reinforce patient confidence in e-Health services… Building trust is a prerequisite to the development of an information society, in e-Health probably more than anywhere else. Citizens prefer services and information tailored to their needs and requirements, while knowing that their right to privacy is protected.”\textsuperscript{205}

The Article 29 Data Protection Working Party has has provided guidance on the interpretation of the applicable data protection with regard to electronic health records.\textsuperscript{206} In its February 2007 working document (on which it invited comment from stakeholders), it noted Article 8 (1) of the Data Protection Directive says Member States shall prohibit the processing of data concerning health. This provision would seem to do away with the possibility of an e-health scheme or, at the very least, electronic health records. However, the Data Protection Directive includes some “mandatory derogations”. Article 8(2)(a) says the prohibition will not apply if the individual has given his “explicit consent” to such processing.\textsuperscript{207} Article 8 (2)(c) also

\textsuperscript{203} Waldo, p. 227.


\textsuperscript{207} The Article 29 Working Party defines explicit consent as “freely given, specific and informed”, which creates a problem for any notions of “implied consent”, as mentioned in the UK context above.
permits processing if it is necessary to protect the individual’s vital interests or where he is physically or legally incapable of giving his consent.

The Working Party notes another possibility allowing the processing of health data:

Article 8 (3) allows for the processing of sensitive personal data under three cumulative conditions: the processing of sensitive personal data must be “required”, and this processing takes place “for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services” and the personal data in question “are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy”.

a) This derogation only covers processing of personal data for the specific purpose of providing health-related services of a preventive, diagnostic, therapeutic or after-care nature and for the purpose of the management of these healthcare services, e.g. invoicing, accounting or statistics.

Not covered is further processing which is not required for the direct provision of such services, such as medical research, the subsequent reimbursement of costs by a sickness insurance scheme or the pursuit of pecuniary claims. Equally outside the scope of application of Article 8 (3) are some other processing operations in areas such as public health and social protection, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system…

Notwithstanding the above, however, the Working Party says Article 8 (4) of the Directive allows the Member States to derogate further from the prohibition of processing sensitive categories of data for reasons of substantial public interest “subject to the provision of suitable safeguards”. The Article 29 Working Party document then sets out its recommendations on 11 topics where special safeguards seem necessary in order to protect individuals’ medical data. These topics are:

- Respecting self-determination
- Identification and authentication of patients and health care professionals
- Authorisation for accessing EHR in order to read and write in EHR
- Use of EHR for other purposes
- Organisational structure of an EHR system
- Categories of data stored in EHR and modes of their presentation
- International transfer of medical records
- Data security
- Transparency
- Liability issues
- Control mechanisms for processing data in EHR.

**Challenges from the private sector**

Since the Article 29 Working Party’s document was adopted, new privacy concerns have arisen in the case of commercial Internet companies getting into the business of providing EHR-type services. Google is offering a new service called Google Health, Wal-Mart and

---

Intel have formed an alliance to offer such services, and AT&T plans a network of health records in Tennessee. Microsoft is already offering a beta version of its health records service, called Microsoft Vault, in a relationship with the Mayo Clinic.209 In the US, medical files in the care of healthcare providers including doctors, pharmacies and hospitals enjoy legal protections specified by the Health Insurance Portability and Accountability Act. Covered files are strictly controlled, can’t easily be subpoenaed, can’t be exploited for profit and have to be stored securely. But Microsoft and Google aren’t health-care providers, as noted in a Washington Post story on the new providers. The Post reporter asks some good questions: “Will consumers have to worry that advertisers will be able to target them so vendors can sell treatments for ailments documented in their records? No, the companies say. Although beefed-up searching for medical issues is a big part of both services, personal files, at least as of now, won’t be taken into account in search results. Both firms also vow that the customers will have total control over their records – no releases without explicit permission. But the very existence of a detailed health dossier accessible in an instant can make control difficult. What if the government subpoenas the records? What if a potential insurer demands to see all the records, telling you that you can’t get a policy if you don’t provide them? What if your spouse – or even someone you’re dating – demands to see all your records?” These are good questions without easy answers.

But another question begs for a response from European regulators. If European citizens opt to use Google Health or Microsoft Vault or other similar offerings, what conditions might the EU seek to impose? And how effective could such conditions be on companies based outside Europe? How will European governments respond to commercial companies offering services that could well become competitive to their own publicly funded EHR systems?210

Need for scrutiny and debate with stakeholders, including the public

The medical profession and policy-makers have not begun to grapple with the implications of companies like Microsoft and Google becoming the hosts for vast stores of patient information.211 Consumer control of personal data under the new, unregulated Web systems could open the door to all kinds of marketing and false advertising from parties eager for valuable patient information.

All these uncertainties lend weight to the recommendation by Waldo et al. that there is an urgent need for a wide-ranging debate on these issues, a debate that involves the public.212

---


210 A spokeswoman for Google Health said the service was a “large ongoing initiative” by the company, which she said she hoped would eventually include “thousands of partners and millions of users.” See Lohr, 20 May 2008, op. cit.


212 An indication of the urgency is the fact that 87 per cent of European doctors already use a computer, 48 per cent with a broadband connection. European doctors increasingly store and send patients’ data such as lab reports electronically. About 70 per cent of European doctors use the Internet and 66 per cent use computers for consultations. These data come from a report prepared for DG Information Society and Media, entitled Benchmarking ICT use among General Practitioners in Europe, Final Report, Bonn, April 2008. [http://ec.europa.eu/information_society/eeurope/i2010/benchmarking/index_en.htm#NEW_Pilot_on_eHealth_indicators:_Benchmarking_ICT_use_among_General_Practitioners_in_Europe](http://ec.europa.eu/information_society/eeurope/i2010/benchmarking/index_en.htm#NEW_Pilot_on_eHealth_indicators:_Benchmarking_ICT_use_among_General_Practitioners_in_Europe)

The survey, while finding high usage of ICT by doctors, did not, however, pose any questions regarding their trust and confidence in national EHR schemes, nor in the adequacy of the protection of patients’ medical data, nor in schemes like those being developed by Google and Microsoft.
Detailed privacy impact assessments, along the lines of that published by the UK Information Commissioner’s Office, would be appropriate too, not just for the offerings by the private sector but for the new EHR systems being established in the Member States. Among the many questions that need to be addressed is whether “implied consent” is indeed being assumed. Some detailed statistical research would help in making such assessments, especially with regard to contraventions and enforcement of the protection of individuals’ medical and health data. Do the EHR schemes, public or private, meet the safeguards set by the Article 29 Working Party? Are new regulations needed to govern contractual relationships involving electronic health records? Should some certification standards be set? How adequately do European citizens understand the implications of the new EHR schemes? Is there a need for independent, third-party audit of the EHR schemes and publication of the results?

Challenges

While electronic health systems offer efficiency and safety gains, they do nevertheless pose several critical challenges as indicated above. Essentially, these include the following:

- How to protect the confidentiality of electronic health records?
- How to avoid secondary uses of data or, if data are to be repurposed, to ensure meaningful consent?
- How to respond to the challenges posed by private sector initiatives such as Google Health and Microsoft Vault?
- How to improve regulatory oversight of the e-health domain and, in particular, to enforce sanctions?
- How to engage citizens in a wide-ranging debate about the implications of e-health schemes?

3.2.5 E-insurance

Insurance markets are strongly affected by ubiquitous computing, for example, by remote measuring technology. Such approaches allow for much better risk calculations, and in effect might lead to better price calculation, from which, in theory, both customers as well as insurance companies can profit. There are different fields of possible application such as the car insurance market, where several insurers already offer black boxes with positioning technology (see section 2.1.2) that can be built into vehicles to track the time and route of driving. Another possible application or obvious extension is the use of “smart” health insurance which computes premiums based on health-conscious behaviour (see section 3.2.4), or personal liability insurance. Until now, there have been only a few deployments by car insurance companies, but a survey by Frost & Sullivan shows that the vehicle e-insurance market in the EU is worth about €2.7 million now, and is expected to grow rapidly over the next decade: they forecast a market value of more than €400 million by 2017.213

One type of vehicle insurance is the “Pay-as-you-drive” (PAYD) model, which is not really that new. Some US states such as Texas and Oregon introduced regulations for such insurance policies several years ago. The PAYD model was expected to reduce the number of uninsured cars owned by persons with low income. It should also be a motivation to reduce car usage for environmental reasons. When first introduced, PAYD was more or less a “pay per mile insurance”, which meant the more you drove, the more you paid in insurance premiums. It

---

was controlled with an “odometer audit”, where the driver had to prove how many kilometres he drove each year. Today, the combination of emerging technologies such as geo-tracking and toll systems allow the use of so-called black boxes, which can register more than just the mileage of a car. The data recorded may include speed, gear, brake usage, fastening of safety belts, lighting, etc. These data can be used by insurance companies to validate their risk calculations and make customer selection or price discrimination towards single consumers or more reasonable towards groups of users with comparable data. Because of this, the development of PAYD is of interest to more than just insurance companies and their customers. Policy-makers dealing with the environment, markets and transportation as well as technologists have an interest in such data too.

Challenges

In contrast to the already mentioned advantages in the social, political or economic field and disadvantages such as customer selection and/or price discrimination, there is a set of possible challenges to privacy caused by collecting, storing and processing data from PAYD schemes.

- The collection and processing of the data allows insurance companies to make more reliable and differentiated risk calculations and, as a consequence, better prices for low usage of cars. This can help to bring people with low income back into the insurance market as well as motivate people to use more public transport, but it can also be misused for price discrimination and customer selection.

- The collection and storage of more detailed data can be used to construct movement profiles. When the driver’s identity is recognised together with car usage data, a detailed profile of the individual’s driving style can be generated.

- The availability of these data will probably lead to the authorities’ wish to use this information not only for accident analysis but also for a wider range of prosecution.

These are a few possible scenarios, but they show the ambivalence of this novel business concerning privacy. Although collecting, storing and processing are inherent results of intended goals like better pricing for car insurance, it is obvious that they also can be easily misused. This statement is not only valid for car insurance; it is also relevant for all other approaches to improve insurance systems by using emerging technologies as shown in the case of e-health (see section 3.2.4). Policy-makers, consumer organisations and other stakeholders need to consider how they should react to the use of new technologies for insurance purposes and, in particular, whether such use may lead to discriminatory practice and, if so, what an appropriate response (or set of responses) should be.

---


3.3 SOCIAL NETWORKS

*Well now we’re respected in society, you ain’t worried ‘bout the things that used to be.*

— “Respectable”, The Rolling Stones

The Rolling Stones tune came from 1978, before the Internet and World Wide Web. If they had written the song some years later, they might have changed the first line, since everyone should be worried about things that used to be or, at least, anything that gets put on the Web: it could be there for a long time and could come back to haunt those whose youthful exuberance and casual attitude towards privacy might become more tempered with age.

Increasingly, the Web is becoming a means for social contact, where communities use it as their main communications channel. Individuals publish information about their own private life and even about others. Such information may become available globally without restriction and may stay visible for an unlimited time. Even when data are removed from the original website, it may remain accessible and retrievable, e.g., in caches of search engines and other information services.

It is an amazing paradox that the same people who react negatively, even with fury, when they discover the details of bank accounts held by 21 million Germans were for sale on the black market for 12 million euros, also provide masses amount of personal data on social networking websites. Social networking websites would seem to serve well both voyeurs and exhibitionists. As a social phenomenon, however, social networking websites pose massive threats to individual privacy.

### 3.3.1 Facebook, MySpace and other social networks

Social networking sites enable users to connect to friends and colleagues, to send mail and instant messages, to blog, to meet new people and to post personal profiles. Profiles include photos, video, images, audio and blogs. In June 2008, MySpace and Facebook each had about 115 million unique visitors a month. Other popular social networks include Friendster, Orkut and Bebo. The Korean Cyworld is reported to have 18 million users, or 40 per cent of the population. Some social networks are dedicated to particular topics, sharing knowledge, or purchases of products and services, or travel itineraries.

---


217 For a more positive view of social networking websites, see the comments made by Viviane Reding, the European Commissioner for Information Society and Media. Among other things, she said that because of the open nature of social networking sites and the fact that they offer cultural diversity and enhanced interactivity, they can serve several different audiences with minimum financial effort and bring about new economic opportunities for European industry. Customer service, advertising, mobile phone industry, human resources, entertainment are only a few sectors that have been changed by the rise of the social networking sites. Social networking sites also turn people into active users of new technologies and empower them to make active choices about their environment by offering the opportunity to create new creative content. European Commission, “Social Networking Sites: Commissioner Reding stresses their economic and societal importance for Europe”, Press release, MEMO/08/587, Brussels, 26 Sept 2008. http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/08/587&format=HTML&aged=0&language=EN&guiLanguage=en


Google and Yahoo have yet to become a force in social networks, though they haven’t given up trying.220

In Europe, 42 per cent of all Internet users regularly use social networking services,221 and more than half (56 per cent) of them visited one or more social networking websites in 2007.222

Most social network sites set a minimum age of between 13 and 14 to create a profile but none actively enforces the age requirement. In fact, there is no easy way to tell whether users are 14 years old or over.223

Social networks are used for a variety of purposes. Many people use them to maintain contact with their friends or to make new ones. A poll of 2,000 adults showed that nearly 30 per cent admitted searching for former girlfriends and boyfriends on the sites, and almost one in three used them to find out about their boss, colleagues or a job candidate. The survey also found 13 per cent of social networkers had posted information about or photos of other people without their consent.224

Some companies use the social networking sites to check out candidates for jobs or for snooping on employees.225 Some companies, including the social network operators themselves, use the sites for data mining and advertising. Companies such as Coke, Apple Computer and Proctor & Gamble use social networking sites as promotional tools.226 Even police forces are using social networking sites.

**Social networkers do care about their privacy**


Helft says Google and Yahoo are trying to turn themselves into social sites without building a social network by linking users’ favourite destination and content, with their friends and communities. Yahoo is attempting “to bring the kinds of features that are common on Facebook and MySpace to its own sites. Users may be able to share photos, videos, news reading habits or calendars with their friends and receive alerts about what friends are up to… One challenge both companies face, however, is how to turn the voluminous amounts of data about relationships that they have in their e-mail, calendar and other services, into ‘social graph’, a set of relationships establishing who is friends with whom. They will have to tread carefully. Google’s efforts to determine who [Google] Reader users wanted to share items with was greeted with some alarm.” Yahoo has said it wouldn’t force relationships on anyone without their consent.


It’s been said, perhaps facetiously, that teenagers often think their lives on social networking websites are private as long as their parents are not reading their online journals.\(^{227}\) The reality, however, is different. Once private information is posted on the Internet, it becomes available for others to read – parents, (future) employers, university admission officials as well as marketers and advertisers, identity thieves, paedophiles and other unsavoury characters.

According to a survey by Pew, 40 per cent said their profile is visible to anyone who happens upon it online.\(^{228}\) Ofcom found almost exactly the same numbers in the UK: 41 per cent of children aged 8-17 and 44 per cent of adults had a profile set so that it was visible to anyone.\(^{229}\) These figures suggest that people are either not so concerned about their privacy or are not aware of the risks in making their profiles accessible to anyone.

Another reason might be that privacy policies on social networking sites have been difficult to find and use. In fact, this is exactly what Ofcom discovered: All users, even those who were confident with ICT, found the settings on most of the major social networking sites difficult to understand and manipulate. Facebook, in particular, was mentioned in this context by a number of respondents.\(^{230}\)

Although they may often be careless with their privacy, people do care about it nevertheless, as shown by the fact that tens of thousands of Facebook members protested against the Beacon “service”, which aimed to tell one’s friends what one had just purchased online. Facebook was notifying users’ friends without their consent. Users protested, saying that Facebook should not be following them around the Web, especially without their permission.\(^{231}\)

### ID thieves harvest personal data from social networking sites

Social networking websites have attracted the attention of ID thieves because of the ease with which they can harvest personal data. A recent Symantec Internet Security Threat Report\(^{232}\) says that just two social networking sites were the target of 91 per cent of phishing attacks with websites hosted in the United States. It also found an increase in sophisticated and personalised attacks on consumers, with personal data most often sold via instant-message groups or Web forums that live for only a few days or even hours.\(^{233}\)

While the potential risk is well documented, Ofcom has said that **there appears to be a lack of research on the actual incidence of crimes such as identity theft as a result of the**

---

227 Barnes.
230 Ofcom, p. 56.
232 The report was published in April 2008. See http://www.symantec.com/business/theme.jsp?themeid=threatreport
publication of personal details on these sites. There also seems to be a lack of research into what UK social networking site users are and are not posting online.234

While the incidence of identity theft has been difficult to quantify accurately, there seems little doubt about the incidence of spamming. About 64 large-scale spam attacks have been reported on social networking sites in the year to mid-2008, and 37 per cent of users have noticed an increase in unwanted messages in the first half of the year, according to Cloudmark, a Web security company.235

Harvesting personal data via applications

Lots of companies are taking advantage of the popularity of social networks to harvest a huge amount of personal information in some ways that are less visible than others. MySpace, Facebook and other social networks are at the disposition of third-party developers of applications. By opening up its code so that third-party developers could write applications for it, Facebook now has thousands of third-party applications (called “widgets”), which, say analysts, have accounted for a jump of about 28 per cent in Facebook’s popularity.236

Every time a user downloads one of these mini-programs, they risk compromising their privacy. People might think that if they set their Facebook profiles and MySpace pages to private, they are only available to friends or specific groups. But that’s not true if they use applications. On Facebook, applications can only be downloaded if a user checks a box allowing its developers to “know who I am and access my information”.

So what do these third parties, who could be anywhere in the world, do with the information? Sometimes they use it to connect users with similar interests. Sometimes they use it to target ads, based on demographics such as gender and age (something Facebook and MySpace also do). Facebook and MySpace say they hold application developers to strict standards. They also point out that some information, such as e-mail addresses and phone numbers, aren’t made available. So far, the issue of personal information going to application developers has had little visibility.237 However, the Center for Digital Democracy is urging the US Federal Trade Commission to look into the privacy policies surrounding third-party applications.238

Deleted, but not deleted

Users of social networks who become concerned about their privacy could always delete their profiles. However, the profiles may not be really deleted. A few Facebook members found that the site keeps profile data intact after users delete their accounts so that they can be

subsequently “un-deleted” if the addictiveness factor of Facebook proves to be too much. The UK’s Information Commissioner’s Office (ICO) said it would investigate what happens to deleted profiles. ICO reportedly believes that the current process of deleting one’s Facebook profile is too complicated and not permanent enough. If Facebook retains the information contained in profiles that users have opted to erase, it may be in violation of data protection laws.

For its part, Facebook says it is committed to working with ICO to maintain a trusted environment and to ensure compliance with UK law. The practice of other social networks with regard to the deletion of information is not known.\(^{239}\)

The big unknown is what happens to all those personal data on the social networking websites. How are they being mined, by whom and for what uses?

**The next big things**

**Mobile social networking**

eMarketer forecasts that *mobile* social networking will grow from 82 million users in 2007 to over 800 million worldwide by 2012. MySpace recorded over 7 million unique visitors to MySpace Mobile in the US in the six months since launch.

It will be necessary to watch how mobile social networking develops, how it is used and how the operators and third-party applications developers make use of it. Undoubtedly, targeted, location-specific personalised advertising will be chief among applications. From a user’s perspective, mobile social networking will offer convenience in connecting with nearby friends, but they may not like intrusive advertising in real-time or subsequently. Those who mine tracking data for where a consumer has been coupled with what he or she has done and with whom he or she has connected will have layers of new data on which to build more personalised “services”, which could also be exploited by real-world thieves who can find out where a user lives and when he or she is out.

*Data portability, including portable profiles*

Google, MySpace and Facebook have all announced plans to enable social network data portability.\(^{240}\)

Facebook announced in early May 2008 the debut of Facebook Connect, a new technology for members to connect their profile data and authentication credentials to external websites. Facebook will handle the authentication process. Although privacy controls have not been made clear, the company has stressed that user security will be a priority.\(^{241}\)


\(^{240}\) There is an open, industry-sponsored DataPortability project. See http://wiki.dataportability.org/display/dpmain/Home

\(^{241}\) A Facebook spokesman said, “Data portability is about much more than data. It’s about giving users the ability to take their identity and friends with them around the Web, while being able to trust that their information is always up to date and always protected by their privacy settings.” See McCarthy, Caroline, “Facebook to open the gates with ‘Facebook Connect’”, CNET News.com, 9 May 2008.
MySpace announced its version, called Data Availability, that would allow users to share personal profiles and other data (including images, video, audio, messaging) across different, even competing websites. The idea is to overcome the hassle experienced by users who are compelled to create a new personal profile every time they register or become a member of different websites.

The MySpace initiative includes Yahoo, eBay, Photobucket and Twitter. MySpace said users will be able to manage how their data are shared and who gets to see them. The MySpace sharing process will use OAuth, an open protocol, which allows information to be passed from one site to another.242

Some analysts say these initiatives indicate “a big shift in how the social networks ... relate to other sites and developers. In the first round, the social networks invited others to make their sites better – widgets on MySpace pages, applications on Facebook. Now the social networks are offering to use the information they have about users to make other sites better, too”.243

Facebook Connect adds another feature. Websites will be able to let users log in and create accounts with their Facebook names and passwords. This is similar to what Microsoft tried and failed to build with its Passport system. The proposed OpenID standard would allow people to log in to one site with an ID issued by another, but it is rather complex and hasn’t achieved the critical mass to be adopted as a standard.

As of June 2008, it is difficult to say how well or quickly data portability will catch on. A month after Google’s announcement about its Friends Connect service, Facebook withdrew from its agreement with Google.244

While these initiatives will benefit user convenience, they also raise privacy issues in sharing personal information across different websites. On the other hand, forward thinkers such as Esther Dyson have been predicting for a long time that we will create a virtual representation of our identities that may help mediate how we connect to (and hide from) others online.245 This is similar to what Second Life and other virtual worlds are talking about too, where an avatar (or digital representation of the user) created in one virtual world can be used in other virtual worlds (see section 3.4.1 above).

Challenges

MySpace, Facebook, Bebo and other social networking sites have faced and continue to face challenges from privacy advocates. A recent one from a Canadian group is typical of the main charges against and challenges facing the websites.246

The Canadian Internet Policy and Public Interest Clinic (CIPPIC) has listed 22 separate breaches of the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA). The basis of the 35-page complaint, filed in May 2008 with the Office of the Privacy Commissioner, says that Facebook collects sensitive information about its users and shares it without their permission. It goes on to say that the company does not alert users about how that information is being used and does not adequately destroy user data after accounts are closed. The CIPPIC said that “if you add a third-party application offered on Facebook, you have no choice but to let the application developer access all your information even if they don't need it... Facebook users need to know that when they're signing up to Facebook, they're signing up to share their information with advertisers.”247

A Facebook spokesperson said it had reviewed the complaint and “found it has serious factual errors, most notably its neglect of the fact that almost all Facebook data is willingly shared by users.”

The Canadian Privacy Commissioner has a year to act on the CIPPC's complaint. The commissioner’s office tries to resolve privacy disputes by negotiation, but it can seek court injunctions if they fail to resolve the issues. This will be an interesting case to follow, to see which if any of CIPPIC’s charges stick and which don’t, and how the Privacy Commissioner decides to resolve the case.

Protecting and regulating data when data are “published”

As noted above, social networking websites provide a rich harvest of personal data for those seeking to exploit such data. Policy-makers face a difficult issue when consumers “publish” or post their “personal data” on Facebook, MySpace and other such websites. Even if they restrict their data, their photographs, information about their interests and values, stories of their experiences to just their friends and families, they are publishing them once they put them on the Internet. Still, the social website operators should live up to their own policies as well as legal policies (e.g., the Data Protection Directive) and social propriety.

Facebook recently came under fire for allowing users to post anonymous comments about other members of the site. By installing the Honesty Box application, members of the social networking site can send and receive untraceable messages to other users. Critics claim that it allows cyber bullying.248

---

3.3.2 Blogging

Along with social networks, blogging is one of the most popular and successful Web 2.0 applications and most of the considerations about privacy and trust in social networks already listed in the preceding section are also relevant here. So, for example, a survey from CareerBuilder, a job database, found that one-quarter of the hiring managers reported that they used search engines to screen job candidates. This includes social network sites as well as blogs and online fora. In addition, the survey found that more than half of managers have chosen not to hire an applicant after viewing their online profiles. Blogging personal data has had other repercussions too. Some employees have been made redundant because they posted internal information. Research has shown that blogging with pseudonyms has not effectively protected one’s privacy.

Due to its open character, as a Web 2.0 precursor application, blogging has affected consumers who have allowed comments on their blogs as well as companies hosting blogging sites. The liability for posts with a racist, discriminatory or other offensive character differs because of different regulations in the various EU Member States. Other problems such as the persistence of blog entries (even after they have been deleted from the original site) or harvesting of personal information have to be considered for blogs in the same way as for social networks.

**Challenge**

The impacts of blogging on privacy and personal data warrant further research.

3.3.3 Social tagging

Social tagging, also known as collaborative tagging, social classification or social indexing, allows ordinary users to assign keywords, or tags, to items. Typically, these items are Web-based resources and the tags become immediately available for others to see and use. Unlike traditional classification, social tagging keywords are typically freely chosen, which has led to the coining of the term “folksonomy”, instead of using a controlled vocabulary or taxonomy. It is one of the earliest Web 2.0 applications and became well known by social bookmarking services such as del.icio.us, which started in 2003. Nowadays social tagging is used by many social networking communities such as Flickr and Facebook, but also by traditional Web offerings such as newspapers and scientific websites. Normally, it is used to tag articles, blogs, photos, profiles and similar things.

Social tagging should help to orientate users and help them to find relevant or interesting information. Online newspapers, for example, use so-called tag clouds to mark graphically the highest rated, most interesting topics or articles.

---

The multi-purpose character of social tagging in the field of information retrieval and knowledge management affects a broad variety of groups. Social tagging is of interest to researchers and librarians because, with a sufficiently large number of tags, useful folksonomies may emerge that can either augment or even replace traditional ontologies. Social tagging is of interest to technologists and Web businesses engaged in the development of the semantic Web because of its possible impact on the information architecture of the Web. This latter aspect is of concern to search engines. Every other type of company can also be affected if they use it as enterprise taxonomies for their knowledge management, as forecast by Millen et al. The social tagging phenomenon could affect all consumers who use existing technologies such as social bookmarks as well as emerging ones such as the semantic Web.

Although social tagging can be used in many environments for different purposes, the basic advantages and problems and, as a consequence, open questions are mainly the same. The greatest advantage is the possible inclusion of all users, which makes it useful as a tool for the interactive development of knowledge. At the same time, the voluntary engagement of users increases the speed of assigning tags, while the costs of doing so decrease. On the other hand, there are many critics, who argue on the unreliable and inconsistent results because of problems like synonymy, homonymy or polysemy.

These problems can be solved in different, mainly technological ways, but critics are concerned about possible misuses by someone assigning irrelevant, inaccurate or denigratory tags, which challenges the balance between trust and privacy. The heated discussions about the services of rottenneighbours.com illustrate these problems in a very clear way. The anonymity and easy access or, in other words, privacy of users, which enables the inclusion of all users, is at variance with the need for trustworthy and accurate entries. One way is to give up the anonymity and introduce systems with several levels of registration and acknowledgment, as Wikipedia has done to deal with the problems it has encountered with the accuracy of articles versus the identification of authors. As Michael Swaine has shown, this balancing between privacy and trust is a general problem for many Web 2.0 applications, especially as long as there are no generally binding solutions or regulations dealing with it.

3.4 SECOND LIFE – A CASE STUDY IN THE CONVERGENCE OF THE REAL AND VIRTUAL WORLDS


254 Morville, Peter, Ambient Findability: What We Find Changes Who We Become, O’Reilly, Sebastopol, 2005.


Second Life bills itself as a virtual world entirely created by its residents. In reality, it is an Internet-based virtual world, developed by Linden Lab and launched in 2003. Users can download a client program called the Second Life Viewer by means of which they can interact with the avatars, or digital representations, of other users. Users (or residents, as they are called) can explore (on foot or by teletransportation or even by flying) this virtual world – or they can trade items, engage in business, advertise products or simply socialise with other residents or, if they are so inclined, have virtual sex with them.

While Second Life (SL) is sometimes referred to as a game, it does not have points, scores, winners or losers, levels, an end-strategy, or most of the other characteristics of games.

By early April 2008, Second Life had more than 13 million registered users, and in the first week of April more than 450,000 of those had logged on to the Second Life website. More than 60 per cent of SL residents are from Europe. (There are more German residents than Americans.)

Many real world companies are marketing their wares to Second Life users. They have bought virtual islands and built virtual stores to hawk their products and services. Billboards have sprung up in Second Life. Some companies such as IBM and Intel have used Second Life for meetings, product development and designing simulated services. Brands such as Adidas and Toyota have created virtual products in Second Life; Edinburgh University has created a cyber campus where students take part in tutorials around a beach camp fire; Reuters has a Second Life reporter; Sweden was the first country to open a virtual embassy in Second Life; the Guardian has hosted a film festival there.

These initiatives indicate how the real and virtual worlds are beginning to converge. Perhaps the best evidence of the increasing convergence is Second Life’s virtual currency, the Linden dollar (Linden, or L$), which one can purchase with a real world credit card. Lindens earned in Second Life can be converted back into real dollars via online currency exchanges (the exchange rate, which fluctuates just like real world currencies, was L$ 269 to US $1 in early May 2008). Residents’ spending also fluctuates, but was roughly in the order of US$1.6 million a day in early May 2008.

Just like real life, Second Life has its share of dubious characters flogging get-rich-quick schemes or defrauding those not paying attention or engaging in de facto extortion. The stock

258 http://secondlife.com/

For a glossary of Second Life terminologies, see http://wiki.secondlife.com/wiki/Glossary

259 “Second Life was pretty much sex-free until residents stealthily seeded in adult content, creating a world where pretty much anything goes. Since then, ‘anything’ has come to include cyber-prostitution, lap dances, orgies, S&M, and the secret trysting places known as skyboxes, which float out of sight high above the clouds.” Wired, “Having Sex”, Issue 14.10, Oct 2006. http://www.wired.com/wired/archive/14.10/slentertainment.html


263 http://secondlife.reuters.com/

exchanges and banks in SL are imposing, but they are unregulated and unmonitored. Investors fed Linden dollars into savings accounts at Ginko Financial bank, hoping to earn the promised double-digit interest. Some did, but in July 2007 there was a run on the bank and panic spread as Ginko ATMs eventually stopped giving depositors their money back. The bank has since vanished. With no official law and order in Second Life, investors have little recourse. Some Second Life residents are calling for in-world regulatory agencies — the user-run Second Life Exchange Commission has just begun operating — and some expect real-world institutions to become involved as the Second Life population and economy expands.265

Ad farms – small patches of land filled with garish virtual billboards – have become a problem. Ad farms obstruct the views of surrounding territory and lower its value. Owners of newly-devalued virtual homesteads argue that the practice is tantamount to extortion, as ad farmers ask for rates well above market value for their land. Large swathes of Second Life’s mainland have been rendered uninhabitable by ad farms, as residents and businesses avoid building next to existing ads.266

3.4.1 Standards

Another sign of the convergence of the real and virtual worlds is the discussion between IBM, Linden Lab and others on open standards that would allow one’s Second Life avatar to roam to other virtual worlds so you wouldn’t have to create a new avatar for every virtual world you visit. Second Life is the best known of the virtual worlds, but there are, of course, others, including IMVU, There, ActiveWorlds, OpenSim, Kaneva and Red Light Center.

IBM and Linden Lab are also planning to offer other companies “secure, flexible and customizable” virtual environments that are designed and controlled by corporations. Currently, many companies are reluctant to let their employees venture into virtual worlds, even though management experts describe Second Life and its competitors as an innovative tool for collaboration among workers, industry partners and customers. But companies worry about keeping the conversations and information secure. The corporate gated communities envisaged in the IBM - Second Life plan, once implemented, would be the equivalent of corporate intranets on the Web.267

3.4.2 Privacy breaches


Authorities have intervened in crimes committed in online worlds. In the Netherlands, a teenager was arrested for stealing more than $5,000 worth of virtual furniture in a world called Habbo. See Hart, Kim, “Virtual Worlds Get Real About Punishment”, Washington Post, 20 Aug 2008.

http://www.washingtonpost.com/wp-dyn/content/article/2008/08/19/AR2008081902706.html

Police in Japan questioned a woman for logging on to the account of a fellow participant and “killing” his avatar after he had “divorced” hers in the interactive game MapleStory, which originated in South Korea, and now has more than 50 million players across the world. Lloyd Parry, Richard, “Jilted Japanese woman questioned by police after ‘murdering’ her virtual husband”, The Times, 25 Oct 2008.

http://www.timesonline.co.uk/tol/news/world/asia/article5008156.ece


Perhaps Linden Lab’s interest in firewalls was stoked by an intruder. Second Life (or Linden Lab, its creator) is as subject to data breaches as any other company. In September 2006, Linden Lab revealed that its account database had been compromised and details of more than 600,000 accounts were exposed. Account names, real names and contact details, but not credit card information, were all visible.268

As virtual worlds consist of ongoing, digital interactions among many individuals, it is only natural to inquire about privacy concerns and how personal information is collected and used. Such questions will become more pronounced as more users venture into the virtual worlds and as these worlds become more commercialised. Some have argued that the inherent structure of virtual worlds impede users’ privacy preferences, while others say that virtual worlds provide users with powerful tools to spread ideas and opinions, thus potentially undermining unfair practices, abuses of data and market failures.269

Privacy International has opined that “‘Virtual existence’ in Second Life implicates real privacy issues, both online and offline, for avatars and their users. In-world concerns include anonymity and reputation of avatars, and the ability to control who is watching, and when. Avatars may be subject to surveillance by Linden Lab, marketers, and perhaps even law enforcement, linking online and offline identities and behaviour in ways that users are often unaware.”270

Optimate Networks (formerly AMPP Media), an advertising company, signed a deal with Linden that allows it to place digital billboards within Second Life. Unlike normal billboards, however, the AMPP billboards serve ads contextually by scanning for keywords in public conversations in their area. These billboards can also serve up adverts to individual residents based on their “interest profile”, which includes a resident’s user information (name and age of account), information on where a resident spends time in Second Life, and even what clothing and attachments a resident currently has on his avatar. The creation and retention of these interest profiles, just as in the real world, raises significant privacy concerns. Privacy International noted that these concerns, however, are especially grave in the context of a virtual environment where individuals’ perceived anonymity leads them to do things they may never consider in real life.

3.4.3 Privacy policy

Linden Lab’s privacy policy says it is committed to protecting the user’s privacy.271 Except under “certain limited circumstances” (e.g., if required by law), Linden Lab says it does not disclose personal information to any third parties without permission. A couple of points are worth noting, especially in view of the controversies that have arisen in social networking (see above section 3.3.1). One of these is that if someone ceases to be a customer, Linden Lab says it keeps a copy of the user’s registration file “in the event the person wishes to rejoin the Second Life service”. Such would seem to be in contravention of European data protection

law (notably the Data Protection Directive and the Data Retention Directive). So the question arises: to what extent can Europe exercise its jurisdiction over a company based outside the Union?\textsuperscript{272} For its part, Linden Lab says that anyone from outside the US using its websites consents to transfer of their data from their country to the US. In other words, if you want to use Second Life, you have no option except to agree to this transfer.

It also says it does not collect information from children ages 12 or younger “because only those individuals who are 13 years of age or older are permitted to register”. (See also the section on social networking for more on this issue.) Registration requires entry of “a valid and eligible date of birth”. But is it possible for Linden Lab to check whether the prospective customer is, in fact, telling the truth? It seems doubtful. In other words, it seems possible for anyone to register as long as they put in a date of birth indicating they are older than 12.

Nevertheless, Linden Lab said it would activate a system to verify the age and country of residence of some users. Under the plan, residents will be required to flag land as “adult” if it contains content that is “overtly, graphically, or explicitly sexual in nature or intensely violent”. Gambling and sexually explicit activities in Second Life are under increasing scrutiny from law enforcement authorities. Linden Lab invited the FBI to examine casinos in Second Life, and German prosecutors have been investigating virtual child pornography. Residents will need to provide passport, driver’s licence or national ID number information to confirm their age and country of residence before being granted access to land flagged as adult by the individual landowners.\textsuperscript{273} How Linden Lab will be able to confirm the driver’s licence, passport number or national ID number was not disclosed. Even if it is able to do so, the issues raises questions about Linden Lab’s compiling a user database with millions of passport or other ID numbers and how securely those data are protected.

Linden Lab warns customers that they should not expect any privacy or confidentiality of any information they disclose to other Second Life users, but Linden does make some suggestions in order to allow users to maximise their privacy in-world. Linden allows residents to choose to appear offline when another resident searches for them and to hide their online status and location, even from other residents who have been added as friends.

3.4.4 \textbf{We want better privacy!}

On the Second Life website, one of the “meta-issues” being discussed is improved in-world privacy.\textsuperscript{274} The bottom line is, as stated on the website, that residents want better privacy and users are urged to “vote for this proposal if you want privacy in any form”. They are invited to leave a comment if they prefer a specific solution.

Among the reasons stated as to why an in-world privacy policy is considered necessary are so that residents can “build in peace or without someone seeing our latest products in development, so we can chat with nearby friends without having to use IMs…, so our homes remain ours, without people wandering around my [virtual] house uninvited…so [there is] …


\textsuperscript{274} https://jira.secondlife.com/browse/SVC-241
no spying!” But it does not seem any easier to establish privacy policies in the virtual world than in the real world – “We’ve been bloody asking for it for years!”, says one resident.

Among the various posted comments are some dealing with security issues, so there is a perceived need to distinguish between security and privacy. Security is seen as pertaining to, for example, the potential for sites to retrieve IP addresses. Privacy is regarded as meaning prevention of access to areas that are currently accessible whether “physically” by an avatar or by abusing camera freedom, i.e., anything that can currently be seen or accessed that users do not wish others to see or access.

One resident is concerned about privacy when a SL client server connects directly to non-SL servers. She says she would like to be asked if she wants to allow a direct connection to a non-SL server.

Another user notes that “Ultimately it’s up to the Lindens, using feedback in the comments for an issue, to decide how something is implemented.”

Yet another resident says there should be two separate privacy meta-issues, one dealing with in-world privacy, i.e., the ability to restrict client access to objects you have “rezzed”275 in-world, including your avatar, the other dealing with real-world privacy, i.e., the ability to play Second Life without exposing information that could be used to identify residents to other players (an issue that would include the user’s address).

The reporter of the privacy blog clarifies that the issue is intended to ensure residents can participate in SL undisturbed by other residents if they so wish. Issues relating to real-life identity are to do with disclosure or data integrity, as with IP addresses. Privacy is anything that people can currently see and/or hear that you don’t want them to see or hear. The reporter says that privacy should encompass whether the user is online or not.

One somewhat frustrated resident comments that the reason why there is no in-world privacy policy yet is because such a policy “does not mean money” (meaning, presumably, that no one makes any money from it).

The above comments show that privacy is an issue in virtual worlds such as Second Life, and despite in-world intrusions and infringements of an avatar’s privacy, no regulatory solutions (virtual or real) have yet achieved consensus and been implemented. One can assume the virtual world’s privacy problems would need to have much greater impact upon the real world before regulators will spend much time considering if they need to do anything.

3.4.5 The terms of service (ToS) privacy policy

Linden Lab’s terms of service contain a privacy policy276 However, in addition to the clauses under the privacy policy, some other clauses in the terms of service make reference to privacy or have privacy implications. A journalist for the Second Life Herald, an independent journal

---

275 “Rez” in Second Life means to create or to make an object appear. Rezzing an object/prim can be done by dragging it from a resident's inventory or by creating a new one via the edit window. The term “rezzing” can also be used for waiting for a texture or object to load, such as “Everything is still rezzing.” or “Your shirt is still rezzing for me.” Taken from the movie Tron's term “de-rezz”, which roughly means to dissolve in a certain way.

not controlled by Linden Lab, wrote a story about privacy in Second Life that generated a comment from a reader who asked, “Are the Lindens to forever remain both judge and jury? Clearly they can act when there is a clear violation of the ToS, but not all cases are so clear-cut. In such cases, is there some due process that one should follow? Do we need, like the real world, to build the infrastructure that interprets the ToS (our constitution) and derives rights and privileges therefrom? Is there a need for 2L lawyers, judges, juries and a system of penalties for those acts that are not outright violations of the ToS but are clearly against the common good?”

Users or residents would not be wrong to view the Lindens as god-like. In the virtual world, as one privacy expert put it, the controllers “can create and store a complete log of all activities and transactions in which the avatar participated, with whom the avatar ‘spoke’ and what was said, every ‘land’ the avatar entered (including the specific time and location), and furthermore, every ‘movement’ the avatar chose to make.” So what happens to all these data? Presumably, Linden Lab is mining and analysing them to “improve the customer experience”, but their possession and power over these data raise concerns about just how intimately they get to know the individual and how these data are subsequently used and protected.

3.4.6 Challenges

With the increasing sophistication and popularity of these online worlds, and with the increasing convergence of the virtual and real worlds, a number of privacy-related challenges may arise, notably:

- Should one’s avatar enjoy the same privacy protection as one’s real self?
- Should real-world regulators be concerned about virtual world privacy issues?
- As with social networking (see above section 3.3.1), is there some way to ensure that children (especially age 12 and under) are either not permitted to register or are not exposed to any risks if they do manage to register successfully?
- As Linden Lab holds personal data and, consequently, is subject to data protection law (such as it is in the US), should it be required to make public the number of privacy-related complaints and comments it receives?
- Should the data protection and privacy practices of virtual world operators such as Second Life be governed by the site operators, the users or regulators?
- Should there be regular audits necessary to check how secure are the personal data held by Second Life and other virtual world operators?
- Similarly, should there be guidelines and/or audits of advertisers’ practices in virtual worlds?
- If standards are agreed so that avatars can roam from one virtual world to another, will their personal data accompanying them be adequately protected?

The risk of certain abuses might be rather high. For example, governments, industry and others might try to profile users based on the data associated with the individual’s avatar, but how far should we assume that an avatar’s behaviour online reflects truly the real person’s behaviour?


278 Zarsky, p. 237.

3.5 CONVERGENCE OF COMPANIES

Companies “converge” in two ways. One is through mergers and acquisitions, e.g., AOL and Time/Warner or Google’s acquisition of DoubleClick. A second way is through partnerships, joint ventures or agreements such as that between Google and Publicis Groupe or that between Phorm and BT. There are many permutations and examples of both types of convergence, just as there are different reasons, different logics for the convergence. The convergence of companies is not a new phenomenon by any means. However, new concerns have been emerging about the convergence of some companies, and those concerns include privacy implications.

In this section, we give some examples of the convergence of companies and then raise some questions about how their convergence might impact privacy. Most of the examples are taken from what has been described as an advertising technology arms race aimed at making digital marketing more effective and pervasive. Some of the examples have received a lot of attention, e.g., Google’s acquisition of DoubleClick, while others are not so well known. All of them involve the so-called new media. All of them raise concerns about personal data, how those data are mined and processed and how the results are used to better target consumers with personalised advertising (see section 3.1.1 above).

The convergence of companies has also been described as a “frenzy” in the online advertising sector as companies try to grab bigger pieces of the lucrative market that continues to grow as more people turn to the Web for their entertainment and information. It can also be regarded as a vertical consolidation between the major Internet portals and/or search engines and/or advertising networks and/or social networks.

The global online advertising market is already huge. Some estimates put it at $37 billion or even bigger and the market is growing fast, indeed, it is growing faster than all other media, including TV and the print media. Part of the allure of the Internet for advertisers is the potential to use consumer data to deliver different ads to different people, based on their behaviour and presumed interests.

The biggest search engines and portals on the Internet – Google, Microsoft, Yahoo and AOL – are all at the forefront of the transformation of the Web, where search engines,
social networks and advertising networks are fuelled by the ready availability of personal information. Together with Rupert Murdoch’s News Corp., they have acquired the biggest social networks, MySpace, Facebook, Bebo and Orkut, as well as YouTube.

In addition to these players, one further example is given, that of Reed Elsevier’s LexisNexis Group’s acquisition of ChoicePoint. Those companies are among the biggest aggregators of personal data.

Today’s battleground is the Internet, but tomorrow’s is likely to be the ubiquitous information society and the embedded world of ambient intelligence. Why do we say that? Because ambient intelligence (or pervasive computing or ubiquitous networking, as it is also known) promises greater personalisation of service through different devices working seamlessly across heterogeneous networks. Personalisation of services requires personal data, as today’s Internet players know very well. The commercial foundations for the brave new world of the future are already being laid.

### 3.5.1 Google’s acquisitions

**AdSense**

Google bought Applied Semantics for $102 million in April 2003. The company provided domain name, contextual advertising and enterprise search solutions. One of its products was AdSense, a program that placed paid listings into web pages, by analysing the content of those pages and then selecting ads that seemed most appropriate. Since then, AdSense has developed into an advertising network, which now serves millions of sites, and is one of the engines of Google’s rapid growth.\(^{285}\)

**Orkut**

Orkut is not so well known a social network as MySpace, Facebook and Bebo, at least not in Europe and the US, but it is well known in Latin America (especially Brazil) and Asia. Nor did Google acquire it in the sense of buying it. Rather, it was developed by Orkut Buyukkokten, a Google software engineer, out of a “20 per cent” project (Google allows, even encourages employees to spend up to 20 per cent of their working time on anything they choose). A beta version of Orkut was released in 2004. Currently, Asia and Latin America account for nearly all of Orkut's 24.6 million monthly users, with just 600,000 in North America and about 1.2 million in Europe.\(^{286}\)

**YouTube**

Google topped Yahoo to acquire YouTube for $1.65 billion in Oct 2006. YouTube is the leader in sharing original videos online. Users upload videos to the YouTube website and thereby across the Internet through websites, mobile devices, blogs and e-mail. At the time of


the deal, YouTube had 72 million individual visitors each month who viewed 100 million videos every day.

YouTube said it agreed to the deal because Google’s ad platform would integrate well into YouTube. It described Google’s platform combined with YouTube’s “innovative technology” as “a perfect match”. In announcing the deal, Google said that its mission is to organise the world’s information and that video is an important part of the world’s information.287

DoubleClick

Google has long told investors that it aims to be a pipeline for all advertising in the future on the Internet and elsewhere.288 To that end, Google announced in April 2007 its proposed $3.1 billion acquisition of DoubleClick, an Internet company that delivers many of the ads consumers see online and which plants many of the cookies on personal computers. According to The New York Times, the deal was “accelerating an arms race among Internet companies seeking a greater share of online advertising”.289

Google’s purchase of DoubleClick stirred controversy for competitive reasons – each company is the leader in its business – and because of the sheer volume of personal information it would concentrate in the hands of one company. The combination of Google’s records of consumers’ Internet searches with DoubleClick’s information from cookies prompted complaints that one company would hold extensive data about a large proportion of the world’s Internet users. In December 2007, according to market-research firm comScore, Google had 62.4 per cent of the worldwide online search market, compared to 12.8 per cent for Yahoo and 2.9 per cent for Microsoft. Google may soon corner the online advertising market, particularly after its acquisition of DoubleClick.290 Google accounted for 28 per cent of the $21.4 billion online advertising market in the United States in 2007, according to eMarketer. In Europe, the market share of Google and DoubleClick is close to 90 per cent in parts of the Internet advertising business, according to some estimates.

The takeover was examined by regulatory authorities in the US, Europe and Canada, but only on competition grounds, not for its privacy impacts.

In December 2007, the US Federal Trade Commission cleared the acquisition. The FTC concluded that the deal was “unlikely to substantially lessen competition” in Internet advertising. Although the FTC did not consider the privacy impacts, it was probably no coincidence that it released its proposed guidelines on behavioural advertising (see section 3.1.1 above) on the same day that it announced its decision.

Microsoft%2C+Yahoo&st=nyt
One commissioner, Pamela Jones Harbour, dissented in the FTC decision, saying that it was too early to know how the online advertising market would evolve and thus too early to know if the deal would threaten competition or consumer privacy.

In March 2008, European regulators followed suit and approved Google’s $3.1 billion acquisition of DoubleClick, brushing aside complaints that the combination would allow Google to extend its Internet dominance.\(^291\) The European Commission said the Google-DoubleClick deal would not hurt competition because Google and DoubleClick occupy different parts of the market, and advertisers would be able to opt for alternatives, including services from Microsoft, Yahoo and AOL.

Google is the leader in small, simple ads which appear on its search pages, while DoubleClick deals with more elaborate display ads, which appear on many sites, and deals in “ad serving”, using software to help advertisers narrow their aim to potential customers.

Critics said the ruling could help create a “digital colossus” by allowing Google to strengthen its position in other kinds of online advertising, including display ads such as banners and television-like video spots.\(^292\)

### 3.5.2 Microsoft’s acquisitions

**aQuantive**

In May 2007, the month after Google agreed to buy DoubleClick, Microsoft acquired DoubleClick’s main competitor, aQuantive, for $6 billion. The price tag was an 85 per cent premium on aQuantive’s closing share price the day before the deal was announced. It was also double what Google agreed to pay for DoubleClick.

aQuantive, based in Seattle, is regarded as a significant player in online advertising and one of the largest buyers of digital media.\(^293\) Its holdings included Atlas Media Console, which serves advertisers by buying and managing online advertising; Drive Performance Media, which buys and resells online ads targeted on user behaviour; and Avenue A/Razorfish, a creative agency, ad broker and one of the world's largest interactive agencies, which works with companies to build websites and the digital marketing programs that drive traffic to them.

The Microsoft-aQuantive deal brought together a media agency that buys advertising space on behalf of advertisers, an ad-serving technology provider and a seller of inventory in MSN. All of which equal vertical consolidation.

In addition to aQuantive and its holdings, Microsoft has acquired several other companies to fill out its digital advert offerings, including Rapt, Inc., which helps website publishers in packaging and pricing display-ad space, AdECN, a stock market-like exchange where

http://www.nytimes.com/2008/03/12/technology/12google.html?ref=technology

\(^{292}\) Castle, op. cit.

\(^{293}\) Mills, op. cit.
networks representing websites buy and sell ad space, and Massive, which inserts ads into video games.\textsuperscript{294}

\textit{AdECN}

In July 2007, Microsoft announced it was acquiring Advertising Exchange Platform AdECN, an advertising network, for an undisclosed sum. AdECN offers a real-time, auction-based, neutral exchange for online display advertising that works in a similar way to stock exchanges. A member of the AdECN exchange buys on the exchange for its advertisers and sells on the exchange for its publishers. AdECN is a direct competitor to RightMedia, a company acquired by Yahoo in April for $680 million. Microsoft said the acquisition would help it to build a comprehensive search and display advertising platform.\textsuperscript{295}

\textit{Microsoft takes a stake in Facebook}

In October 2007, Microsoft acquired a 1.6 per cent stake in Facebook, at a cost of $240 million.\textsuperscript{296} The transaction valued Facebook at $15 billion. The deal gives Microsoft control over the placement of banner ads on Facebook outside the US, where about 60 per cent of Facebook’s 49 million active users reside.\textsuperscript{297}

\textit{Yahoo (not)}

On 1 Feb 2008, Microsoft announced an offer of $44.6 billion for Yahoo, a price that dwarfed that which it paid for aQuantine, which was already larger by three times the price it had paid for any other company. \textit{The New York Times} described it as “a bold move to counter Google’s online pre-eminence” in search and advertising as the computer world shifts from desktop products to online software and services supported by ads.\textsuperscript{298} The story quoted Jon Miller, the former chairman and chief executive of AOL: “No one can compete with Google on their own anymore.”

With the Yahoo bid, analysts said, Microsoft was trying to buy a big enough share of the market to be a credible alternative to Google with online advertisers.\textsuperscript{299}

Yahoo has spent billions of dollars in recent years to develop better search and advertising technology, but its growth has lagged. Microsoft also lags far behind Google not only in online search and advertising, but also in “cloud computing” (see section 3.2.1 above) where


\textsuperscript{296} Microsoft paid almost half of what NewsCorp paid for the whole of MySpace, which is a much bigger social network.


Google leads in offering online software services, including Web-based alternatives to Microsoft Word, Excel and PowerPoint.\(^{300}\)

Microsoft, analysts say, finds itself in a battle where improving its search algorithms and online ad software is not enough. Google’s edge in search traffic attracts more advertisers and Web publishers, so each advantage reinforces the other, in what economists call “network effects”. One measure of the network advantage, analysts estimate, is that Google collects 40 to 100 per cent more revenue per search than either Yahoo or Microsoft. In the most recent quarter, Microsoft had online revenue of $863 million, compared with $4.8 billion at Google.\(^{301}\)

In early May 2008, Microsoft raised its offer to $47.5 billion equivalent to $33 a share, while Yahoo held out for $37 a share. Microsoft walked away from the deal.\(^{302}\) When the stock exchange opened up the following Monday, Yahoo’s shares dropped by 20 per cent, to $23.31.\(^{303}\)

3.5.3 Yahoo’s acquisitions

Overture

In 2003, Yahoo bought Overture Services, the company that pioneered search advertising, in a $1.63 billion deal, to counter its rivals Google and Microsoft, in the expanding market for Web search advertising. Yahoo said the deal would allow it to expand its pay-for-performance search business and to expand contextual advertising throughout its network. Overture specialises in selling advertising links that accompany search results on sites such as Yahoo and MSN.\(^{304}\)

Right Media

Yahoo acquired RightMedia, the online advertising network, for $680 million in April 2007. Yahoo had previously bought 20 per cent of the company for $45 million in October 2006. The acquisition was regarded as a counter to Google’s acquisition of DoubleClick.

RightMedia runs an advertising marketplace that allows for much more efficient advertising pricing than older negotiated models. RightMedia works with large intermediate ad brokers and addresses the “short tail” of the ad market (as does DoubleClick), unlike Overture and Adsense whose “long tail” products address many smaller advertisers and publishers.\(^{305}\)

---

\(^{300}\) Lohr, 2 Feb 2008, op. cit.

\(^{301}\) Lohr, 2 Feb 2008, op. cit.


BlueLithium

In September 2007, Yahoo acquired BlueLithium for $300 million. BlueLithium is the fifth largest ad network in the US and second largest in the UK. Specialising in behavioural targeting, the company analyses data from the 145 million monthly online visitors worldwide who are exposed to its adverts to help advertisers reach consumers with appropriate interests.

In a statement, Yahoo CEO Jerry Yang said BlueLithium’s products, technology and people would help his company in its effort to build the leading online advertising platform. “This acquisition will extend our ability to deliver powerful data analytics, advanced targeting, and innovative media-buying strategies to our customers, who are increasingly looking for these insights. By leveraging BlueLithium’s complementary expertise and tools, we will be able to better address the needs of our performance-based display advertisers and enhance the value of our publishers' inventory.”

3.5.4 AOL’s acquisitions

Advertising.com

In 2004, AOL bought online ad network Advertising.com for $435 million. Ad.com operated the industry’s largest third-party advertising network, with more than 110 million unique visitors a month. It had operations in the US, the UK, France, Germany, Norway, Sweden and Denmark. The company buys ad space from 3,000 sites and resells it to about 500 clients, employing technology to steer ads to the users most likely to act on them using its proprietary AdLearn technology.

Most of Advertising.com’s business came from distributing adverts for customers who pay on a performance basis. Pay-for-performance advertising has proven to be a lucrative market for Yahoo and Google. According to AOL, pay-for-performance media accounted for a greater share of online advertising than CPM (cost per thousand of ad impressions) for the first time in the fourth quarter of 2003. In the Web’s beginning, advertisers paid publishers based on the number of people who saw the adverts. Google and Yahoo built a cost-per-click model, where advertisers pay for an ad only when a Web surfer clicks on it. Ad.com’s special twist is that it charges most advertisers only when a consumer takes a real action – buying something or giving the advertiser a phone number for a follow-up call.

AOL also saw online users moving away from subscription portals (such as its own) to search technologies (such as Google’s), which lets people find and visit so-called “long tail” or niche sites that they wouldn’t otherwise be aware of. It became the first portal to buy an ad network and, through Ad.com, began selling ads on other sites.

Prior to purchasing Ad.com, AOL only sold ads on AOL.com, other company-owned sites and the flagship AOL service. By contrast, Google was selling both on Google.com and on sites owned by partners.

Tacoda

AOL bought Tacoda for a reported $275 million in July 2007. Tacoda developed technology to serve adverts based on the websites a user visits. Ad.com employees were reportedly working on similar technology and some opposed the purchase. 309

Quigo

AOL bought Quigo Technologies for a reported $350 million in November 2007. Quigo sells contextual text ads, the small, sponsored links that run next to articles. Historically, AOL earned its revenues selling Internet connections and subscriptions to its online service, but has since changed its focus to selling Web advertising. Quigo is the third advertising network acquired by AOL in the last few years, and the deal highlights AOL’s goal of selling ads across cyberspace rather than simply on its own websites. AOL executives are trying to turn their company into a one-stop shop, via its Platform-A division, for advertisers that want to reach customers throughout the Internet. 310

Bebo

AOL bought teen social networking site Bebo for $850 million in March 2008. At the time, Bebo had about 40 million users. 311 It is ranked the second most visited in the UK, number one in Ireland and New Zealand, and number three in the US. Bebo was the world’s ninth most popular social networking site in January 2008, according to the Internet statistics provider comScore. 312

AOL said Bebo recognised that the Internet is less about destination and more about connecting people, culture and lifestyles. 313

With Bebo, said one analyst, AOL “plunged head first into the red-hot social networking space, albeit a space that has yet to establish a long-term advertising model”. AOL said that Bebo's audience meshed well with its instant messaging platforms, AIM and ICQ, which reach about 80 million users. 314

Social networking sites are a valuable resource for online advertising, because members post information about themselves and can then be targeted with products and services likely to appeal to them.

3.5.5 News Corp’s acquisition of MySpace

In July 2005, Rupert Murdoch’s News Corp bought Intermix Media, owner of MySpace, then the fifth most-viewed Internet domain in the US, for $580 million. Some said Murdoch was getting “a gold mine of market research, a microscope into the content habits and brand choices of America’s capricious youth market – not to mention millions of potential new customers for News Corp.’s Fox subsidiaries.” It might well have been a gold mine: News Corp estimates that MySpace is now worth more than $15 billion.315

At the time, Murdoch said MySpace would drive traffic to his Fox TV sites.

Earlier in 2005, then New York State Attorney General Eliot Spitzer accused Intermix of deceptive business practices, including the use of spyware that delivered pop-up adverts and redirected users to its search engine. Intermix agreed to pay $7.9 million to settle the suit but did not admit wrongdoing.316

3.5.6 Reed Elsevier’s takeover of ChoicePoint

In February 2008, Reed Elsevier, owner of the LexisNexis Group, announced that it was seeking to acquire commercial data broker ChoicePoint. According to The Washington Post, the $4.1 billion deal would create a “global information-gathering powerhouse that would collect and analyse billions of records about who people are, where they live and with whom, and what they own”.317 With customers including government agencies, insurance companies, banks, rental apartments, corporate personnel offices and private investigators, both companies have played key roles in law enforcement, homeland security and intelligence.

ChoicePoint itself has bought dozens of companies to become an all-purpose data broker. In 2004, it acquired Seisint, an information service, which created a controversial tool called the Matrix, which gave state and federal authorities new power to analyse records about Americans. In recent years, ChoicePoint has focused on refining data with analytical software.

Privacy advocates said the proposed acquisition raises significant issues for regulators. Marc Rotenberg, executive director of the Electronic Privacy Information Center (EPIC), told the Washington Post, “Increasingly, this is less about what big business knows and more about how business uses information to make decisions about consumers. Both of these companies are having an increasing say over the opportunities that are available to consumers as well as to decisions that restrict individuals.”

Rotenberg said the companies are able to sell very detailed profiles of individuals to businesses, insurers, government agencies and others, but individuals do not currently have a right to see what information about them is being sold to third parties.

Quite apart from what the companies do with personal data, both have been the victims of data thieves and have had run-ins with regulatory authorities. ChoicePoint disclosed in February 2005 that thieves posing as small business customers gained access to the company's database, possibly compromising the personal information of 163,000 Americans. In January 2006, the company agreed to pay $15 million to settle FTC charges that the data warehouser's security and record-handling procedures violated consumers’ privacy rights. In 2007, the company settled with 43 states over allegations it failed to adequately secure consumers’ personal information. The company agreed to adopt stronger security measures, and to pay $500,000 for public education campaigns about identity theft. It later settled shareholder lawsuits prompted by the incident. In a smaller incident in 2005, LexisNexis disclosed that hackers got access to personal information as many as 32,000 U.S. citizens in a database owned by LexisNexis.\footnote{Associated Press, “Reed Elsevier Buys ChoicePoint for $4.1B”, 21 Feb 2008. http://ap.google.com/article/ALeqM5hNc2YWd77EMBJntBx_9q2h8be1iQD8UUPF580}

### 3.5.7 Partnerships

**Google and Publicis Groupe**

Google and Publicis Groupe announced in January 2008 that they were working together to develop advertising technologies. The two companies had already been collaborating quietly for about a year, but are now hoping to extend that relationship. The Paris-based Publicis Groupe is one of the world’s largest advertising groups\footnote{The London-based WPP, which criticised the deal, is one of its chief rivals.} and the first major player in traditional advertising to publicly embrace Google. Publicis owns the Saatchi & Saatchi ad agency as well as media planning and buying operations including ZenithOptimedia, Digitas (an online advertising company acquired for $1.3bn in December 2006), Zed, Starcom and Fallon.


Google CEO Eric Schmidt said that “possibly hundreds” of Google employees could take placements within Publicis. While Schmidt and Levy spoke of a partnership, one perhaps cynical observer said it would be anything but, since it was unlikely that Google would give any special knowledge to Publicis.\footnote{Danick, Jackie, “Google, Publicis, and the small matter of Performics”, Latitude, 25 Jan 2008. [Latitude, based in the UK, bills itself as “one of the world’s largest and longest established search marketing agencies”]. http://www.latitudegroup.com/weblog/permalink/google_publicis_and_the_small_matter_of_performics/}

**Yahoo and WPP**

In May 2008, Yahoo announced a partnership with the WPP Group, the advertising holding company, which will give WPP’s clients a broader range of websites where they can aim their
messages. \(^{322}\) Under the deal, the thousands of Web publishers that use Yahoo’s advertising auction service to sell space on their sites will get more direct access to WPP’s clients. Those clients, in turn, will be able to direct their messages to website visitors who might be particularly receptive, using technology from an ad-targeting division of WPP called 24/7 Real Media. WPP’s clients will also benefit from the extra information the agency will be able to collect about the behaviour and demographic profile of people who visit sites on the Yahoo auction service, which is called Right Media. Those details will enhance the database that GroupM, which is WPP’s flagship planning and buying agency, collects about customer behaviour.

3.5.8 Challenges

The rich troves of data collected by the biggest Internet companies are creating a new kind of digital divide within the industry. Traditional media companies, which collect far less data about visitors to their sites, are increasingly at a disadvantage when they compete for ad dollars.

Some advertising executives say media companies will have little choice but to outsource their ad sales to companies such as Google, Microsoft, Yahoo and AOL to benefit from their data.

Even with all the data Web companies have, they are finding ways to obtain more. The giant Internet portals have been buying ad-delivery companies like DoubleClick and Atlas, which have stockpiles of information. Atlas, for example, delivers 6 billion adverts every day. \(^{323}\)

The “convergence” of companies that have significant volumes of personal data and/or the ability to reach consumers raises many questions:

- Do acquisitions of such companies create companies with dominant market power that could be injurious to the public interest?
- Should such M&As be scrutinised in terms of their acquisitions of personal data?
- Is it adequate to scrutinise such convergence only in terms of competitive effects? Should such deals or alliances also be scrutinised in terms of their privacy impacts?
- Should sales of personal data be reviewed by regulatory authorities and/or the consumers whose details are being sold?
- What guarantees do regulators (if not individuals) have that third parties acquiring such data will protect it adequately or not abuse it in contravention of EU legislation, notably the Data Protection Directive?
- Does the convergence of companies, examples of which are referenced above, lead to new uses of personal data for purposes not originally foreseen (and certainly not by those from whom the data have been collected) when the data were collected originally?


3.6  CYBER CRIME (INCLUDING DATA BREACHES) AND ITS COSTS

Data breaches and losses, through ID theft, negligence and carelessness, are not a new phenomena, but they are growing. Thus, government, industry and stakeholders need to consider what additional responses or efforts can be made to curb these losses that have soaring social and economic costs, including the undermining of trust and confidence in government and industry and in participation in e-commerce and e-government schemes.

3.6.1  Breaches and losses of personal data

The past year, from mid-2007 to mid-2008, has surely been an *annus horribilis* for the UK government. The biggest disaster was in November when the Revenue and Customs agency revealed that the personal data, including names, ages, addresses, national insurance numbers and bank account numbers, of 25 million people had gone missing. A month later, in December, the transport ministry admitted it had lost personal information relating to more than 3 million learner drivers. Nine National Health Service trusts also mislaid information on hundreds of thousands of patients. Every week or two seems to have brought news of yet another loss. The most recent (as of September 2008) was an admission by the Ministry of Defence that the records of 900,000 serving and ex-service RAF personnel, contained on three portable hard disk drives, had been stolen.324

The UK Commissioner’s Office (ICO) said government departments and private companies have reported an “alarming” number of new data breaches in the wake of the Revenue and Customs fiasco. Two-thirds of nearly 100 data breaches reported to ICO were committed by government departments or other public sector bodies, with unencrypted information lost on laptops and computer discs, paper records and memory sticks lost, stolen or missing in the post. Missing material included personal data such as health and financial records. Data were recovered in only three cases. Breaches included one at the Ministry of Defence, where an unencrypted laptop containing personal information on 600,000 potential recruits was stolen. The Driving Standards Agency lost records of 3 million people who sat driving tests.

The private sector still accounted for a third of the reported breaches (many more may have gone unreported). In one of those cases, HSBC, one of the UK’s largest banks, lost a disk containing the personal details of 370,000 customers.325

Although the public sector losses (and more like them) were horrible, there have been even larger data disasters in the private sector. They include the 2003 theft of 92 million e-mail records from Internet company AOL and the illegal access in 2006 of more than 94 million credit and debit card accounts through the systems of TJX, the US discount retailer. The latter case seems to be the largest data breach in history. Canadian privacy officials concluded an eight-month investigation into the breach by faulting TJX for failing to adequately safeguard customer information.326

---

If anyone thinks that the blame for the loss or abuse or breach of personal information can be laid only on the doorstep of government, big business and cyber criminals, they would be well advised to review a report based on investigations by the ICO and the police. They uncovered evidence of a widespread and organised undercover market in confidential personal information. The report details how the unlawful trade in personal information operates: who the buyers are, what information they are seeking, how that information is obtained for them, and how much it costs. Interestingly, among the ultimate “buyers” are journalists. Other cases have involved finance companies and local authorities wishing to trace debtors; estranged couples with one party seeking details of their partner’s whereabouts or finances; and criminals intent on fraud or witness or juror intimidation. The “suppliers” almost invariably work within the private investigation industry.327

3.6.2 Incidence and costs of cyber crime and data breaches

The incidence and costs of cyber crime and data breaches are the subject of regular reports and studies, with the most alarming statistics reported in the news media. In the following paragraphs, we draw attention to some of these reports. One could quibble about differences and inconsistencies between these various reports, but, in our view, the most important point to note is the trend. Are the numbers of attacks and breaches increasing? Are the costs of privacy breaches to individuals, companies and government department growing? In the following paragraphs, we refer to some recent reports.

Symantec’s latest Internet Security Threat Report328 is interesting because it highlights the differences between sectors. In the previous six months, the education sector accounted for 24 per cent of data breaches that could lead to identity theft, more than any other sector. Government was the top sector for identities exposed, accounting for 60 per cent of the total, a significant increase from 12 per cent in the first half of 2007. Theft or loss of a computer or other data-storage medium was the cause of most data breaches that could lead to identity theft during this reporting period, accounting for 57 per cent of the total. It accounted for 61 per cent of the identities exposed in the second half of 2007, more than any other sector.

An even more recent report says the data breaches in the US as of August 2008 had exceeded the breaches for the whole of the previous year.329 The Identity Theft Resource Center of San Diego, which issued the report, said the true number of records affected is likely far higher, because many businesses are not reporting data breaches or are not aware of them.

APACS, the UK payments industry association, reported that online banking fraud losses rose by 185 per cent to June 2008 over the 2007 figure, to total £21.4 million during the six
months to June 2008. APACS blamed the increase on criminals targeting online banking customers through phishing and spyware scams. The number of recorded phishing attacks increased, with more than 20,000 fraudulent phishing websites set up in the first half of 2008, 180 per cent an increase more than the same period in 2007.330

ICT-related crime already has a significant impact on businesses, governments and organisations around the world. To take the UK as one example, IT security problems have now become a fact of business life with more than two-thirds of businesses experiencing at least one security breach in the last year, the most common being viruses (68%), staff misuse of IT systems (64%), fraud or theft (49%) and unauthorised access by outsiders (39%). The average UK business now receives roughly 20 viruses a year (rising to 50 for large businesses) and has its website scanned or probed many times. Although the average seriousness of security breaches has fallen slightly since 2002, the number of incidents has increased, so the total cost to UK business continues to run into billions of pounds.331

In the US, the Computer Security Institute (CSI) Computer Crime and Security Survey reported that the average annual loss reported by US companies more than doubled to $350,424 in 2007. Financial fraud overtook virus attacks as the source of the greatest financial loss. Virus losses, which had been the leading cause of loss for seven straight years, fell to second place. Another significant cause of loss was system penetration by outsiders. Almost one-fifth of those respondents who suffered one or more kinds of security incident said they had suffered a “targeted attack”, i.e., a malware attack aimed exclusively at their organisation. Insider abuse of network access or e-mail (such as trafficking in pornography or pirated software) edged out virus incidents as the most prevalent security problem, with 59% and 52% of respondents reporting each respectively. When asked generally whether they had suffered a security incident, 46% of respondents said yes.332

Data security breaches are a costly problem for companies, both financially and in terms of reputation. The Privacy Rights Clearinghouse, a US not-for-profit group, has identified more than 215 million records of US residents that have been exposed since January 2005 because of security failures. According to the Ponemon Institute’s 2007 Annual Study: Cost of a Data Breach, it now costs companies almost $200 per customer record compromised in a security breach.333 The average cost per record compromised is up 43 per cent since 2005. Yet even as

the problems expand, there is increasing evidence that many companies simply do not take them sufficiently seriously. A survey of US and British businesses published in December 2007 by Kroll On-track, an information management company, found that fewer than half of the businesses in both countries had a strategy or policy in place on how to deal with electronically stored information.334

The numbers in the preceding paragraphs deal with the incidence and costs of cybercrime and cyber attacks, but some more academic studies have begun to analyse the costs of privacy breaches, especially on companies’ share prices.335 Acquisti, Friedman and Telang show that there exists a negative and statistically significant impact of data breaches on a company’s market value – which is what one would expect. Unfortunately, there is no such indicator for privacy breaches that occur in government, but that does not mean there is no indicator at all. A drop in public trust and/or confidence in government is one indicator. Indeed, following the several widely reported breaches or losses of personal data in the UK in 2007 and early 2008, there has been a significant drop in public trust. According to a survey of more than 1,000 UK residents, Data Encryption Systems (DES) found that 90 per cent did not trust the government with their personal data.336

These reports and others like them are timely reflections of public concern. Clearly there is greater public, corporate and political interest in data protection and its associated costs than ever. These studies are also useful in suggesting indicators and metrics, which in turn are useful in indicating areas where improvements are necessary and in indicating that governments and corporations ignore privacy and data protection concerns at their peril.

3.6.3 Growing sophistication of cybercrime

Cyber criminals are adopting the software industry’s new service-based model. In the last few years, more software, such as e-mail, word processing, spreadsheets and so on, has been moving online in a trend towards “software as a service” (SaaS, see section 3.2.1 above). But now computer-security firms say criminals have adopted the new model too, and are offering “crimeware as a service” (CaaS). Security guru Bruce Schneier says cyber criminals are moving upmarket, and now they are real businesses. A few years ago, they were selling e-mail addresses, credit-card numbers and other personal information. Then they began trading information about weaknesses in computer systems and selling software kits to exploit them. More recently, they began renting out botnets, huge groups of hijacked computers, infected with malicious software. The new offerings allow criminals to use and pay for such nefarious services via a web browser.337

Phishing scams have grown a lot more convincing and sophisticated. “Two years ago, they were easy to spot because they were littered with spelling and grammar mistakes. Now, the

websites really do look like the real thing,” said a spokesperson for APACS, the UK payments industry association.  

Spam has always been a form of cybercrime, but lately it has permutated and it is now finding a more personal route to afflict consumers: the cellphone. Compared with spam e-mail, junk text messages are seen as more invasive because the cellphone is more intimate and is used for one-on-one communication – a quality marketers are trying to utilise.  

Spam is often a nuisance, but more malicious messages can lead to a new form of fraud called smishing, which uses spammed SMS (text) messages with phishing. Smishing attacks disguise themselves as legitimate messages from e-commerce or financial sites such as eBay, PayPal or banks, and seek to dupe consumers into giving up account numbers or passwords.

3.6.4 Prosecutions

The number of perpetrators successfully prosecuted is rather low. In the UK, Experian has said only six per cent of ID theft cases reported to police currently result in prosecution. 

Even this low level might be high compared to other countries. A US think tank said in an August 2008 report that law enforcement authorities are doing little to resolve what has become a $7.1 billion problem in 2007. The report, prepared by the Center for American Progress (CAP), in collaboration with the Center for Democracy and Technology, said that in the 20 states that give a number for consumer complaints, there were roughly 20,000 Internet-related complaints in 2007, stemming from spyware, viruses and phishing. The National Association of Attorneys General’s bimonthly Cybercrime Newsletter for 2006 and 2007 mentioned just 55 prosecutions of Internet fraud, 26 related to online sales or services, 15 related to data security or identity theft and 14 involving spyware, spam or phishing.

3.7 Privacy and Trust

Effective protection of personal data and privacy is a necessary precondition for users’ trust and confidence when using the possibilities and tools of the Information Society. In addition, further conditions have to be met. Using the Internet for transactions, be they commercial or administrative or of any other nature, the user depends on a number of providers of services who all contribute to making the transaction possible. In addition to the user and the final vendor or service provider, this includes providers of electronic communications services and networks, web hosting, portal providers, directories, online shops, payment service providers, authentication services and several others.

In order to trust the complex system enabling Web transactions, the user must have confidence that all parties involved comply with a set of reasonable rules, not only relating to

---


data protection and privacy but also to an acceptable business practice in a more general sense.

This level of confidence is often not present. Many surveys indicate that many consumers refrain from online transactions because of concerns over the trustworthiness and the overall complexity and lack of transparency of the suppliers of online products and services.

Lack of trust, often based on negative experience, blocks many businesses, in particular SMEs, from reaping the full benefits of online commerce. E-commerce has great reach, it is relatively easy to address an audience wider than any other media and the lower costs of doing so are clear advantages over traditional media. Nevertheless, the difficulty of achieving a relationship with the potential customer based on confidence in the fulfilment of the mutual liabilities is an obstacle to investment in Information Society business opportunities for many enterprises.

As the Information Society becomes increasingly ubiquitous, as things become embedded with RFID and networking sensors, it is inevitable that our everyday behaviour and actions will leave data traces in complex networks. If there is minimal transparency about what is happening to these data trails, citizens will exhibit a corresponding lack of confidence in using online services and may oppose new developments that might potentially create huge benefits for the economy and society.342

3.7.1 Surveys show a lack of trust

In a recent survey of 27,000 randomly selected citizens in the 27 EU Member States, Eurobarometer found that two-thirds said they were concerned as to whether organisations that held their personal data handled these data appropriately. Most European Internet users feel “uneasy” [Eurobarometer’s word] when transmitting their personal data over the Internet: 82 per cent of Internet users reasoned that data transmission over the Web was not sufficiently secure.343

In the United States, the Center for the Digital Future in the Annenberg School at the University of Southern California has been tracking a representative sample of the American population for several years. Of their latest Digital Future Project 2008 report, they say, “Privacy and security online have been found to be major concerns in each of the seven Digital Future studies. Almost all respondents have reported concerns about the privacy of their personal information when or if they buy on the Internet… Overall concern was the highest since the first year of the Digital Future Project.”344

342 Extracted from the privacy and trust tender specifications.
It is interesting to note that the Eurobarometer survey was somewhat at variance with the UK survey (carried out by Data Encryption Systems). According to the Eurobarometer survey, 36 per cent UK citizens did not trust UK tax authorities to use their personal data in the proper way, while the DES survey found, as mentioned above, one in 10 had no confidence in the UK government. This huge difference could be accounted by the fact that the questions were framed somewhat differently.
We can assume that the public’s low level of trust, especially with regard to the handling of their personal data by government and industry, undermines public support for e-government services and the flourishing of e-commerce.

3.7.2 What is trust?

Trust, like privacy, is a rather fuzzy word, meaning different things to different people. Nevertheless, we can characterise trust and make some observations about trust, as in the italicised text below, which would (we assume) be accepted by most people.

We can say that trust is the glue that binds society together. As such, it is a core societal value. Without trust, society would quickly become dysfunctional. Political and social institutions would crumble without the foundation of public support. The economy would be reduced to barter. The notion of friendship would disappear.

Fortunately, most societies have sufficient trust to function, grow and even prosper. But even in the most advanced countries, people are wise not to trust their institutions and systems implicitly. To be completely trusting is, to put it charitably, to be naïve.

We can trust other people, institutions, systems, information, ourselves and probably other things too. If we trust any of these, it means we have confidence that they will behave or perform as we expect even though trust implies the presence of some uncertainty or risk.

There are degrees or shades of trust. You might trust your best friend to return the tenner you lent him for metro fare, but you might not trust him enough to give him an unsecured loan of a quarter of a million to buy a summer home in Costa Rica. Similarly, in the online world, you might not trust a website you’ve never heard of to make good on a purchase of a wall-size plasma TV, but perhaps you would if you were buying the same product from Amazon with a million life-time ratings of 99.5 per cent. Trust is thus a function of what is at risk.

If nothing bad happened when you made your first purchase from Amazon using your credit card, then it is likely you will have more confidence the second time. If Amazon was the first website where you used your credit card and everything worked okay, then you are more likely to have confidence in eBay and some other websites too, maybe even some you have never heard of before. Probably you will have more trust in a website with a trust mark and positive ratings from other users. Over time, you become more trusting of e-commerce. In this way, we can say a feature of trust is that it accumulates. It becomes like (and, indeed, is) social capital.345

If, however, you begin online banking and become victim to phishing, then your trust in e-commerce may go down. And no matter how many times your bank says it has improved security controls, you will still be sceptical about trying e-banking again. Thus, we can say that trust is fragile, easy to damage, difficult to rebuild.

345 Angela Sasse says something like this: “Trust is an integral part of our social and business interactions: trust that is warranted will, over time, lead to an increase in social capital and a decrease in the cost of economic systems.” Sasse, M. Angela, “Usability and trust in information systems”, Cyber Trust & Crime Prevention Project, UK Office of Science and Technology, London, June 2004. The Social Capital Foundation defines social capital as “a resource that can be used to revitalize social cohesion, and can be defined as a set of mental dispositions and attitudes favoring cooperative behaviors within society”. www.socialcapital-foundation.org.
Trust is also context dependent. You might trust someone to mend your car, but you might not trust him with your child’s education.346

### 3.7.3 Online trust

Interactions in cyberspace are riskier and require more trust than similar interactions in a physical context. In addition to having to trust the trustee, users have also to be prepared to trust the technology that mediates interaction (for example, the Internet) and their own ability to use both the underlying technology, and the specific application (for example, the e-commerce website) correctly. For the last two factors, usability is a key prerequisite.347

Guerra et al. identified three main aspects of trust in electronic transactions as identity, privacy and security: “The potential for difficulties in establishing the authenticity of the identity of a consumer or online business is one of the characteristics that distinguishes trust issues in electronic environments from most other contexts. For consumers, identity is bound up with concerns about privacy and data protection.”348

Concerns about online trust can be characterised in at least two ways. One is with regard to the trustworthiness of the online world, the hardware, software, user interfaces, communications links and architecture. Online trustworthiness was the subject of an excellent, somewhat technical report from the US National Research Council, entitled *Trust in Cyberspace*.349 The book asks: Is the trust we place in networked computer systems justified? And if it isn’t, what can we do to make such systems more secure? The book provides a detailed assessment of the current state of the art for building trustworthy networked information systems, and proposes new directions for research in computer and network security, software technology and system architecture.

The second concern is over the success of e-commerce if consumers are fearful that they will be cheated, defrauded, have their credit card numbers stolen, receive poor quality goods, or if businesses stay away fearing costly losses from actions such as failure to pay, repudiation of their commitments and so on.350 There is evidence to support the common sense view that distrust of the Internet undermines e-commerce.351 Robert Gellman claims the costs incurred by both business and individuals due to incomplete or insufficient privacy protections reach tens of billions of dollars every year. He says, for example, analysts estimate that Internet retail sales lost due to privacy concerns may be as much as $18 billion.352

---


347 Sasse, p. 12.


350 Nissenbaum, p. 103.


Online trust especially involves trustworthiness which is related, but not the same as trust. Trustworthiness can be defined as the property of a system whereby it does what is required and expected of it – despite environmental disruption, human user and operator errors, and attacks by hostile parties – and that it does not do other things. Trustworthiness has many dimensions, including correctness, reliability, safety and survivability, in addition to security.353

3.7.4 Factors that shape trust

The Eurobarometer survey mentioned above indicated that the level of “concern” (let’s say trust) about the protection of personal data varied by age and level of education. Respondents from the youngest age group (15-24 years old) were least likely to say they were concerned about the protection of their personal data (53%), while the 40-54 year-olds were the most concerned (69%). There was a clear trend that the higher the level of education, the greater the concern that personal data may not be treated properly by the responsible organisations. Similarly, there was a difference according to occupational status, with manual workers and the unemployed less concerned than employees and the self-unemployed.354 The level of concern also varied by country, with citizens of Germany and Austria much more concerned than citizens of Netherlands (86 per cent v. 32 per cent).

The Eurobarometer findings would seem to be at variance with an analysis of data from an Oxford Internet Survey in the UK, which led Dutton and Shepherd to conclude that generational, educational and geographical differences did not shape online trust so much as experience did.355 From their analysis, it seems that those exposed to the Internet gain more trust in the technology. They found that the levels of cybertrust are related to an individual’s patterns of use or non-use of the Internet over time.356

While there may be differences of opinion about which factors most shape trust, we can, nevertheless, identify several factors that shape online trust to some greater or lesser extent, as follows:

History and experience – The first is that mentioned above by Dutton and Shepherd, i.e., positive experience in the past (you got what you ordered from Amazon) makes trust more likely in the future.

Reputation and endorsements – Even if one has not had direct experience in e-commerce, the positive reputation an online company has in the views of other users induces trust. If the website has been endorsed by the government or a civil society organisation, then we are more likely to trust that website than others without such endorsement. Ditto if the website has a trust mark from VeriSign.

“Lack of trust is one of the most frequently cited reasons for consumers not purchasing from Internet vendors.” The authors provide an integrative review of the empirical literature on trust in e-commerce.353


354 Eurobarometer No 225, op. cit., p. 9.
Image, appearance, stated values – Even if we have no opinions from other users, we may trust an online company by virtue of the design of its website and any stated or implied values. In other words, the company may look trustworthy (even if it isn’t).

Guarantees – The website company may induce trust by offering money-back guarantees or offers of free use of its product or service for a 30-day trial period.

Membership – The online company may belong to an association with a stringent code of practice which is sufficient to convince us that the company can be trusted.

User friendliness, ease of use, clarity of information – If the online company’s product or service is difficult or complicated to use, it may lower our trust or confidence. If the company’s privacy policy reads like a complicated legal document (apologies to lawyers), then we may have doubts about how much confidence we should place in the company.

Balance of power, information asymmetries – If we perceive the online company as having overwhelming power (compared to our own) – e.g., if we want the product or service, we have to agree to all of its conditions, or the company may not have any competitor offering a comparable product – we may automatically distrust the company. If we perceive an information asymmetry – the company has much more information than we do and is not forthcoming, e.g., with regard to how it uses the information we supply – we may also distrust the company. A long-term study of e-commerce showed that consumers’ trust is related to their understanding of how information about them is treated; it wanes if they think that it will not be held in confidence.357

Guerra et al. say that uncertainties make the establishment of identity very important in e-commerce transactions, in order to determine who you are dealing with, verify his reputation and create accountability. Data collection can help trust by creating a legal bond between the parties involved. However, the collection and availability of data can create problems of trust in terms of privacy because individuals may be wary of data surveillance, or of the secondary use of that information. Indeed, privacy is repeatedly identified as a concern that prevents consumers from using the Internet for transactions.358

3.7.5 Trust busters

We can identify at least five categories of trust busters, i.e., those who damage or destroy our online trust.


Other authors such as Angela Sasse have identified still other factors that determine whether users are prepared to trust and engage in an exchange: (1) the number of actors involved in the exchange (ranging from two to potentially millions); (2) the actor type (individuals, organisations, technology such as an e-commerce web site); (3) whether there is synchronous or asynchronous trust exchange (asynchronous exchanges create higher strategic insecurity); (4) whether the user can identify trust-warranting properties; (5) the type of signals employed to communicate trustworthiness (symbols and symptoms of trustworthiness, identity and property signals); (6) the trustor’s propensity to trust; (7) the trustor’s knowledge of the situation; (8) the trustor’s prior experience; (9) the potential benefits expected by the trustor; and (10) the risk to the trustor’s risks (enacted as ‘trusting action’). Sasse, M. Angela, “Usability and trust in information systems”, Cyber Trust & Crime Prevention Project, UK Office of Science and Technology, London, June 2004, p. 12.

358 Guerra et al., p. 4.
First are those evil-doers bent on phishing, distributing malware, setting up botnets and stealing our identities, i.e., those who deliberately break the law to gain access to our personal data and our assets. Not only are we right to distrust evil-doers, but also we may distrust their victims: If a bank or online merchant has been victimised by these evil-doers, we may avoid that bank or merchant because we are afraid that if we use the victim’s website, we may become a victim too.

Second are those who are simply careless or negligent with our data such as government and industry who do not put in place adequate security to protect our personal data and who fail in their fiduciary duty (whether that duty is legalised on paper or not, it is “legalised” in our perceptions) to take adequate care of our data. Trust in the UK government’s ability to protect our data has taken repeated hits since Revenue and Customs lost records of 25 million citizens in October 2007.

Third are those who sail close to the edge, those nominally law-abiding enterprises that want our personal data and want to do whatever they can to process them in order to convince us to buy more of what they have to sell. “The behavior of today’s commercial Web providers is responsible for these attitudes… Nearly 63% of consumers who decline to provide personal information to Web sites report it is because they do not trust those who are collecting the data... 86% of commercial Web sites provide no information of any kind on how any demographic data collected will be used, or even whether data is being collected.”

Fourth are the law enforcement authorities and security agencies, the counterparts of the third group, who want as much of our data as possible so they can check whether we indeed are law-abiding or whether we belong to a terrorist cell. We may not trust this group because we are not convinced that they are using the data they collect for the stated purpose. If they are found to be spying on ordinary, law-abiding citizens without a court-authorised warrant, our trust in them will suffer.

Fifth are the insiders (friends, relatives, neighbours, co-workers). We may trust these people more than anyone else, but most security breaches come not from evil-doers trying to break into a system, but from those in a position of trust.

When the actions or failures of any or all of these groups come to light, they damage our trust in what we can do online. Repeated failures (for example, by the UK government) make us wary of any new e-government “services”. Hence, no matter how much a national electronic health records scheme or national biometric identity database might benefit us, there is strong

---


360 Excessive surveillance can undermine trust. If, as in London, we are being surveilled all the time, we can draw two conclusions. One is that London must be a very dangerous place if so much surveillance is required. A second is that the government does not trust us. But the government’s distrust in us works reciprocally. If the government does not trust us, why should we trust the government? See the comment made in the Surveillance Society report for ICO: “All of today’s surveillance processes and practices bespeak a world where we know we’re not really trusted. Surveillance fosters suspicion…how far can this go? Social relationships depend on trust and permitting ourselves to undermine it in this way seems like slow social suicide.” Ball, Kirstie, and David Murakami Wood (eds.), A Report on the Surveillance Society, for the Information Commissioner by the Surveillance Studies Network, September 2006, p. 3. http://ico.crl.uk.com/files/Surveillance%20society%20full%20report%20final.pdf
opposition because we don’t trust them, we are afraid they will fail yet again in protecting our personal data.

3.7.6 Trust models

We can look at different trust models and see what works and what does not. Broadly speaking, there are two types of trust models – one is where the consumer-citizen has a choice to engage in an interaction where he needs to trust the other (or others) involved in the transaction, while the other is where the consumer-citizen does not have a choice (e.g., he must file a tax return and he is forced to trust the government not to lose or abuse his personal data).

In each transaction involving trust, we need to identify
- the actors,
- what each hopes to gain from a relationship involving trust,
- what is being exchanged,
- under what conditions, and
- what are the risks.

The actors in the interaction need to identify and assess the risks even though they do not have complete information (which is why some trust is necessary to make the exchange or interaction work). There are two main types of risk. First is the risk that the other is not reliable, that he will not behave as we expect or hope. Second is the risk that the network across which the transaction takes place is not reliable, e.g., evil-doers are able to intercept the transaction or to spoof the other’s website.

Trust models where the consumer-citizen has choice

We can identify several trust models where the consumer-citizen has choice. Here are a few examples.

Reputation model

Amazon makes an interesting case study in trust. Consumers trust Amazon. It has grown like topsy (by about 35 per cent in 2007, with revenues of $15 billion). It has developed a successful business with diverse products.

Amazon has been described as “the ultimate e-tailer, a company that has blazed a trail in business-to-consumer e-commerce”. Industry experts attribute its success to an obsessive focus on customer satisfaction, an emphasis on personalising the shopping experience, innovative technology and business practices. Experts say Amazon has earned its customers’ trust by consistently providing secure transactions, reliable fulfilment and shipping, broad product selection and price discounts. Amazon.com has excelled in using past purchasing data to personalise customers’ shopping experience, modifying pages on the fly to individuals' preferences and interests. It encourages customers to post product reviews as an aid to others.

Moreover, Amazon “has managed to do this in a way that most customers perceive as useful and not as a creepy surveillance practice.”

Consumers see how others have rated (five stars is the best) the products for sale by Amazon as well as the suppliers who do business through Amazon. It has successfully encouraged consumers to provide comments on their purchases. It has a clear, readable privacy policy (which you can find by clicking on the small print at the bottom of the screen) even if you disagree with aspects of it. While consumers trust Amazon, it is interesting to note that Amazon has succeeded even as it stores consumers’ credit card numbers and their past purchases in order to create profiles of individual users and to target them with personalised advertising (“As someone who has shown an interest in memory sticks you might like to know about the following offer.”).

Amazon represents a trust model based on user ratings (reputation). The principal actors are Amazon and the consumer. The consumer wants a product (let’s say a book) sold by Amazon. The consumer must identify himself. In the way of personal data, the consumer must provide his name, address and credit card details (number, expiry data, security code, name on card). The consumer has to determine and assess the risks of buying a book from Amazon, of giving Amazon his personal data, of the link between the consumer and Amazon and how well or badly we think Amazon will protect our data or whether Amazon might use our data for some purpose other than in completing our purchase of the book. In view of the huge number of positive ratings Amazon has received from other consumers, of Amazon’s privacy policy, of the fact that Amazon uses secure socket layer (SSL) for taking our data, we decide the risks are small and we decide to go ahead with the purchase.

**Transparency, opt-in model**

An opt-in model offers a high degree of transparency and would virtually force prospective users to see an explanation of its services and give them an explicit choice about whether to participate or take up those services. E-government services, especially, should be structured this way – i.e., the user has a choice whether to use online government services (for example, in filing a tax return electronically). The service provider (the government, in this case) would still offer alternatives (e.g., in filing a paper-based tax return).

**User control model**

In social networks (in theory), one can choose with whom we wish to share our information, e.g., just our friends and family or others with similar interests or anyone in the world. In this model, there are various actors, principally the consumer-citizen, the social network itself (e.g., Facebook or MySpace or other) and the other people with whom we decide we will network. There may also be a legion of third-party applications developers. In this case, we are posting and maybe even exchanging some personal data, but we decide what that information will be. It could be our CV, a resume of our last holiday, some photos we took of the Parthenon when we went to Athens, or our favourite recipe for walnut brownies or whatever. In exchange for this information, we get the convenience of sharing our latest experiences with all of our friends or family all at once, which gives us a certain amount of pleasure or fun. It may stimulate our friends or family or anyone else with similar interests, e.g., anyone else who has taken a holiday in Athens or anywhere else that might be of interest.

---

to us in deciding where we will go on our next holiday. Since we decide what information we want to supply and with whom, we decide that the risks of using Facebook or MySpace or other social networking website are relatively small and decide to do so.

Trust models where the consumer-citizen has no choice

In some models, we are compelled to trust the other, where we have no choice but to supply some personal data. Most, but not all of these models or cases involve governments. Essentially, there are two types of models. The first is where we must take some action to supply the personal data, the other is where we do not have to take any action, but our personal data are captured anyway. Here are some examples:

Examples of where we have to supply personal data

In some cases, we are compelled by law to supply personal data to the government, and we are forced to trust the government (even though we may not) to protect our data and not to abuse them.

- The UK government (and it is not alone) intends that all residents must have a biometric identity card and/or passport. For the card, we will need to supply some personal data (e.g., our name, address, date of birth, etc.) as well a digital image of ourselves and our fingerprints.
- All taxpayers with taxable income must file a tax return, which can be done online.
- All citizens and residents must respond to census questions.
- Typically recipients of social services, including social (financial) support, must supply personal data in order to receive the service, including income support.
- The UK government has decided that all health records must be digitised and held centrally.
- And so on.

Examples of where our personal data are captured or exchanged without our consent

In other cases, our personal data may be captured legitimately but without our knowledge. Every time we leave our homes, CCTV cameras are tracking us wherever we go. One could argue that such video is not personal data, but we would argue that it is. It is an image of ourselves, even if the CCTV operator does not know our name, where we live, etc, but the day is coming when facial recognition algorithms will be able to correlate our image with other data and determine who that is in the leather jacket going down the steps into the metro station.

Law enforcement authorities and intelligence agencies may be capturing our personal data without our knowledge, mining and processing such data in order to determine whether we are car thieves or terrorists.

Credit-checking agencies such as Experian also gather our personal data without our knowledge or consent. We can check those data and dispute their accuracy, but the data are being collected and exchanged whether we like it or not.
3.7.7 Trust strategies

Where the citizen-consumer is compelled to provide his personal data, where he has no choice but to do so, or where his personal data are gathered without his knowledge or consent, it should come as no surprise that he is less likely to trust the data controller (the entity that has his data) than cases where he voluntarily provides his data, whether that trust is misplaced or not.

Google Health and Microsoft Vault may succeed better than the UK’s own electronic health record scheme simply because the user has choice.

Governments can create more trust (or perhaps more support) for their data collection schemes by being more transparent, by adhering to the EU Data Protection Directive, indeed going beyond the requirements of the Directive. They can say how they will use the data they collect. They can submit to third party audits and on-the-spot, unannounced inspections (e.g., by the data protection authorities), with the results to be made public. Individuals who work for the data controller as well as the data controller as an entity could be punished in some way where there has been a dereliction of care. The affected citizens could receive restitution.

Governments can submit new data collection schemes to public consultation. They can also create and invite independent advisory committees and/or the data protection authorities to carry out privacy impact assessments to determine the least intrusive approach, whether there are alternatives to the scheme or the way in which some schemes are to be implemented. All stakeholders should be invited to comment on the schemes.

3.7.8 Challenges

Need for more empirical research

There is only a weak empirical foundation for assessing the basis upon which people are prepared to trust others in cyberspace or to trust in the trustworthiness of ICT systems. 363

Although there have been numerous articles and books about trust generally and trust in relation to ICT, Bennett and Raab say that we need to know more about the dynamics of trust in different contexts involving regulation, self-regulation and technology-based privacy instruments. 364

Need to support users in making the correct trust decisions

Since trust is a critical factor for user acceptance of cyber-systems and their long-term success, it has prompted a spate of research on human-computer interaction (HCI) and computer-mediated communications (CMC). Most of this research aims to help those designing or deploying such systems: the focus is on increasing users’ trust perceptions, rather than allowing users to make correct trust decisions. 365


365 Sasse, p. 12.
Need for some systematic handling of trustworthiness issues in systems development

Systematic handling of issues of trustworthiness is not at all widely established in the systems development community. In particular, there is no stable, shared notion of a “liability and responsibility structure” that can be used in systems development. This is an emerging area, and a focus for development and education. The lack of this understanding can have major negative consequences in the roll-out of new technologies for trustworthy systems.366

Need to develop and understand online trust strategies

The fact that many users distrust e-government and e-commerce shows that both government and industry need to develop more robust strategies to convince the consumer-citizen that he or she can engage in such services safely and in confidence.

In a paper prepared for the OECD, Guerra et al. said there are still many uncertainties around the definition of trust in relation to the use of ICTs, such as the Internet, and in developing strategies for enhancing consumer trust in e-commerce. “Moreover, there is debate over whether e-commerce might be undermined or enhanced by the adoption of certain strategies designed to enhance trust. The rationale for seeking to develop strategies to enhance trust, including the use of privacy-enhancing technologies (PETs), online alternative dispute resolution (ADR) procedures and other products and services, is sometimes based on the belief that increased trust will reduce overall transaction costs and risk. At the same time, the growth of e-commerce could be inhibited by particular approaches to enhancing trust, for example, if strengthening the level of privacy protection or identification procedures is achieved using methods that create unacceptable increases in costs or operational burdens. Finding an appropriate framework that balances the need to offer consumer protection while maintaining e-commerce growth involves many interrelated uncertainties: economic, psychological, institutional, technical and legal.”367

Need for empirical evidence on how the Internet and other ICT impact trust

Guerra et al. say that empirical evidence relating to the precise impact of the Internet and other ICTs on trust is still sparse and sometimes contradictory,368 a point reiterated by Dutton and Shepherd: Empirical evidence relating to the social dynamics determining the impact of ICTs on trust is still sparse and contradictory.369

366 OST, Ibid., pp. 18-19.
368 Guerra et al., p. 4.
369 Dutton and Shepherd, p. 435.
4 CHALLENGES FROM ADMINISTRATIVE DEVELOPMENTS

4.1 E-GOVERNMENT – INTRODUCTORY REMARKS

E-government has become a major topic in recent years for most municipalities, states and other institutions. European institutions and Member States are increasingly investing in e-government systems, including electronic identity systems (e-ID), electronic voting, health care, etc. Although some of these developments (for example e-health in section 3.2.4) are already mentioned and analysed in other sections of this report, we give a short overview here of the general problems and challenges facing these developments and then exemplify them with different important applications.

A first major problem results from the different uses of terms such as e-government, e-democracy, e-governance or e-administration, which are often inconsistent or even misleading. Therefore, the terms used in this section need to be defined first. All-embracing in this case is e-governance, which means governance in the Information Society. This includes all areas of life and society, in business as well as politics. The political domain and administrations embrace e-government (in a narrower sense), which is aimed at modernising and improving public services, and e-democracy, which is aimed at improving public participation in the decision-making processes within a democracy and, as a minimum, taking better account of public opinion.

Another major problem from the point of view of this report is that the question of privacy and trust in e-government is related to several administrative levels and matters concerned by initiatives and regulations in this field. On the one hand, these levels vary from a municipal and state level, for example, in the case of taxation, to an EU level in the case of cross-border procurements or even up to an inter-state level, for example, in the case of passenger name records. Another dimension is the integration of private suppliers in the form of public-private partnerships as, for example, in Austria, where mobile or bank cards serve for transactions between citizen and state. On the other, the purpose of these measures varies as well, from simplifying administrative processes such as tax declarations to tracking criminal activities, such as money laundering.

A third problem is the variety of related functions, which can be addressed by e-government applications, and their complexity. The range varies from applications such as e-consultations and cross-border e-procurement on an EU level, which are realised in a lot of Member States to more advanced areas like public registries, which are only partly realised in some states. The reasons for this heterogeneous development are the differences between the requirements, concerned rights and regulations in each country. The analysis of different developments in the Member States, where some Member States only have begun to start e-government applications, while other Member States already working on solutions for a range of

---

370 There are inconsistencies, even within the European Commission, in the spelling of these terms. In some cases, for example, e-health, e-Health, E-Health and eHealth appear in the same document. Although the only “e” example given in the New Oxford English Dictionary for Writers and Editors is “e-commerce” (lower case), we have chosen to follow that style of spelling for other similar terms such as e-government, e-democracy, etc. (except where some other spelling variant is part of a title or a direct quote). The exception is e-ID since, by itself, ID is often used as an abbreviation for identity.

administrative functions, points to the fourth problem.

This gap, which is mentioned in the case studies in the “Breaking barriers to eGovernment” report, is the result of two interrelated elements. One is the existing system of administrative data storage and processing in the states (administrative context). This is influenced by citizens’ attitude towards state authorities and especially their trust in the reliability of data processing, storage and use. The Scandinavian countries, which are most often considered to be the advanced states in this area, are good examples for this. In the late 1960s, Denmark and the other Scandinavian countries introduced, after a positive popular vote, a so-called CPR number as a personal identification number, which consists of a 10-digit number (six digits for the date of birth and four digits as an individual number). Within this process, all personal administrative data about a person, which were held before at the municipal level, were merged into one central data storage, which was turned into an electronic database located in a state-owned data processing centre. All data concerning a person from the registration, social security, health system and tax are held together there. This development was possible because, in the Scandinavian model of the welfare state, it was widely accepted that the state held such data in return for the security it provided to citizens.

Public acceptability is not restricted to the state as shown by the example of Sweden where registration lists and income tax declarations are public. In total, the system of single identifier and single database allows the use of the CPR number for several electronic purposes, from applications for unemployment insurance benefits to borrowing books from public libraries. Comparable developments for legal as well as cultural reasons are unthinkable in other Member States. For example, Germany ruled some years ago that a single identifier would be unconstitutional.

Because of both the growing significance of the topic as well as the argument that e-government projects do not always pay sufficient attention to privacy and data protection, there is a lot of research going on in this area. Due to this and the aforementioned problems, we have limited the scope of our analysis. As a first step, we outline the main challenges of e-government applications. As a second step, we analyse some e-government applications to show the challenges and to depict the described problems.

In general, most studies, including the report “Breaking barriers to eGovernment”, indicate a lack of trust because of fears about inadequate privacy and security and indicate deployment of safeguards as a key challenge to be addressed before these systems can be successfully implemented. They also show that these concerns and fears exist within every group of potential users – only the depth of concern differs. One of the most interesting facts is that

people who already use online banking and comparable systems seem as reluctant to use e-government systems as non-users, although these systems often have safeguards lower than most of the e-government projects. To explain this attitude, many of the studies note several, interdependent factors behind these concerns, but a common finding in all is the already-mentioned lack of trust.

**Challenges**

The reasons for lack of success most often cited in the different studies may be categorised as follows:

1. Some studies stress the fact that e-projects do not pay enough attention to the privacy concerns of users, i.e., users of e-government services often feel left alone without support or assistance and don’t understand the security and privacy guidelines and technologies of such systems.

2. Users are concerned that data from e-government and/or e-democracy systems might be accessed by unauthorised third parties including cyber criminals.

3. Perhaps the most frequently mentioned apprehension about e-government is citizens’ fear of a Big Brother society in which state authorities themselves make unauthorised secondary use of collected and stored data.

All of these fears interact with other problems that confront e-applications, such as negative publicity about poor co-ordination, technological and design flaws, poor usability or leadership failure. Although private companies also have these problems, it seems that the public sector has more such problems or suffers from more bad press. These reasons and interactions set the stage for the challenges to privacy and trust which we now discuss in more detail in the context of the following applications.

### 4.2 Biometric Identity Documents and Electronic Identities

People can prove they are who they say they are by various means, but the most common is by production of a passport or identity card or similar documents like a driver licence. In this field, two highly interrelated developments take place, which raise a crucial series of challenges.

One development is the introduction of electronic identities for citizens within EU Member States, on EU level itself or other countries. The aim of electronic identities is to ease the communication with administrations, for example, to apply for unemployment benefits or file tax returns. This raises several issues, because the collected data could be accessed by different administrations or a third party. This spectrum of possible purposes has led to a development where some states try to improve the security of such systems by basing them on biometric identity documents.

---


379 Klüver, Lars, Walter Peissl, Tore Tønnes et al., op cit.
The introduction of biometric identity documents itself is mainly reasoned with a series of security arguments, including prevention of identity fraud, curbing immigration abuse, illegal working and organised crime, and ensuring that public services are only used by those actually entitled to them as well as with arguments on usability. But RFID-embedded, machine-readable documents make the task of gathering information much easier, because data can be stored and/or combined or linked with other data to build better profiles of individuals for different purposes.

4.2.1 State of the art

Due to the above described convergence of biometric identity documents and electronic identities, it is nearly impossible to make a clear distinction between both developments. As a consequence, we want to analyse firstly the international standards and agreements on identity documents. In a second step, we will briefly summarise what has been done so far in both areas on the European level and then describe examples from several Member States, which cover both electronic identities and biometric identity documents. Finally, we give an outlook on developments in non-EU states.

International standards

Most countries have identity document schemes, but as yet there are no internationally agreed standards for identity cards so that a citizen of one country could use his or her identity card in another country. In some countries, the possession of an identity card is compulsory while in others it is voluntary. Usually if you have a passport, you do not need an identity card.

Virtually everyone who travels from one country to another needs a passport, except in the EU where an identity card is sufficient for EU citizens. The International Civil Aviation Organisation (ICAO) agreed standards for machine-readable, biometric passports in July 2005. ICAO’s 188 Contracting States agreed that all must begin issuing the machine readable passports by no later than 1 April 2010. Most already do so. ICAO chose facial recognition as the primary biometric with iris and fingerprints as backup (but not compulsory).

At the European level

In the European Union, the Council adopted Regulation (EC) 2252/2004 on security standards and biometrics for passports and other travel documents issued by Member States in order to strengthen the link between the passport and its holder on 13 Dec 2004. On 28 Feb 2005, the Commission adopted the first part of the technical specifications which relate to the storage of the facial image of the holder on a contact-less chip. On 28 June 2006, the Commission adopted a second Decision relating to the additional storage of two fingerprints on the passport chip.

---

381 Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, OJ L 385, 29.12.2004. Article 1.2 says “Passports and travel documents shall include a storage medium which shall contain a facial image. Member States shall also include fingerprints in interoperable formats. The data shall be secured and the storage medium shall have sufficient capacity and capability to guarantee the integrity, the authenticity and the confidentiality of the data.” The storage medium of choice is an RFID chip.
The EU also plans to collect the fingerprints and other biometric data from all visitors to the EU and in the process the Visa Information System (VIS) will become one of the world’s largest biometric databases. The VIS is a system for exchanging visa data between Member States and is expected to help in preventing people from entering the EU illegally or overstaying their visas. The Council decided to establish the Visa Information System, purpose and structure in February 2004.\footnote{382} The Council and European Parliament reached agreement on the VIS regulatory package in June 2007.\footnote{383}

The VIS Regulation will allow consulates and other competent authorities to use the system when processing visa applications and to check visas. The VIS Decision will allow police and law enforcement authorities to consult the data under certain conditions aimed at ensuring a high level of data protection. The Visa Information System will store data on up to 70 million people concerning visas for visits to or transit through the 15 European countries that have so far signed the Schengen treaty of 1985 to end internal border checkpoints and controls. These data will include the applicant’s photograph and 10 fingerprints. The VIS will become the largest 10-fingerprint system in the world.

The EU measures would replicate many of the border checks in the United States, but would go further in requiring EU citizens to submit fingerprints or other biometric identifiers to participate in computerised, fast-track, entry-exit customs controls. Visitors would also have to register within an electronic visa system similar to one used in Australia, which gives travellers an electronic travel authorisation when booking their flights. The online system would record travellers’ names, how they paid for the voyage and their destinations – information that would be checked against European databases of blacklisted people.\footnote{384}

In a further step, the European Justice and Home Affairs Council approved minimum security standards for national ID cards in late 2005, a step on the way towards a European biometric ID card. These standards adopted for ID cards are those already adopted for the European biometric passport, which is based on the ICAO standard, which consists of an RFID chip containing a digitised photo and fingerprints of the passport holder. As a result of the fact that Member States base their electronic identities more and more on these ID cards, the process of convergence will go on.

In the field of electronic identities itself, the European Commission announced in May 2008 a three-year pilot project aimed at cross-border recognition of national electronic identity (e-ID) systems in 13 Member States. The new system will allow citizens to identify themselves electronically in a secure way and deal with public administrations either from public offices, from their PC or any other mobile device. The Commission says easy access to public services across the EU is crucial for citizens travelling within Europe for business, studies or holidays and contributes to the mobility of workers.

This e-ID project, called STORK (Secure idenTity acrOss boRders linKed), will build on existing systems and try to find common specifications that can be further developed and gain

wider agreement. The EC and participating partners are funding the project to the tune of €20 million. According to the Commission, some 30 million citizens already use national e-ID cards to access public services such as claiming social security and unemployment benefits or filing tax returns.

**EU Member State experiences**

While the introduction of biometric passports is or will be finished soon in most of the EU Member States, they differ strongly in the implementation of electronic identities. Some countries, notably the Scandinavian and Baltic countries, France and Italy, have already introduced electronic identities. Several other countries have started pilot projects in this area. Some of these e-IDs are independent solutions, while in other cases they are based on ID or signature cards, which are sometimes secured with biometric data. In view of this variety of developments, we present only some example cases.

In the Nordic countries, single personal identifiers eased the introduction of electronic identities. In the case of Denmark, for example, it is nearly impossible to open a bank account or borrow a book from a public library without this personal identifier, called a central personal registry (CPR) number. An official ID card does not exist. In reality, the national health insurance card took over the position as a document although it not contains a picture of the card holder or any other data. Nowadays, the card with the CPR number and a PIN code allows people to apply online for unemployment benefits or loan books from public libraries. In Finland, the development is one step further. In 2001, the so-called FINEID (Finish Electronic Identification) was introduced, which combines a national ID card and an electronic signature card. The card displays name, sex, date of birth, nationality and social insurance number, but these data are not stored on the chip. The chip itself only contains the Finnish unique identifier and the signature. While the introduction of the card was widely accepted, it has raised criticism in recent years because of the low spread, high costs and few applications. In contrast to Finland, where the card is voluntarily, in Estonia, a comparable approach of integrating electronic identity with national ID card is obligatory for citizens and foreigners, who have a residence permit for more than one year. Unlike in Finland, the card also contains a picture and more information is stored on the chip (the unique identifier, name, signature/authentification). Even more information is stored on the Belgian ID card, which was introduced in 2005 after a successful pilot project. It stores the complete data, which is printed on the card (including the picture) and electronically on the chip as well. The photo, however, does not include biometric information. However, in each of the cases (Finland, Estonia and Belgium), the chip is prepared to include this information in the future. The step of storing biometric information on a combined national ID card and electronic ID card is already done in Italy, which introduced the so-called Carta d’Identità Elettronica (CIE), on

---


which biometric data from photo and fingerprints are stored. In several other EU Member States, it is still a point of discussion if new versions of ID cards should also work as electronic identities and if they should include biometric data. France has a non-compulsory ID card, and plans for replacing it with a new combined card, which were announced in 2007, are still being discussed. In the Netherlands, where an ID card has been compulsory since 2005, the discussion on electronic IDs has also started. The UK has begun introduction of an ID card, which includes biometric data, similar to the Italian approach.

Some other countries decided not to integrate electronic identities with ID cards for several reasons. Most advanced is the case of Austria, where ID cards are not obligatory and therefore not very widespread. The so-called “Bürgerkarte” (citizens card), which allows the use of electronic signatures and authentication, can be integrated in other chip-based cards, for example, bank cards, mobile phones or students cards. The Austrian eID system also integrate the possibility that eID cards from Finland, Italy, Belgium or Estonia can be utilized within the Austrian system to use the services. In other countries, such as Slovenia or the Czech Republic, pilot projects have started, exploring the option of integrating electronic identity functions at least partly into newly issued health insurance cards.

All these examples from the different EU Member States show that a broad variety of electronic identity systems as well as of national ID cards, both with or without biometric data, already exists. At the same time, it highlights the need for initiatives like STORK, which try to harmonise the different electronic identity systems. Furthermore, it also shows that regulations are needed on minimum security standards for national ID cards such as the already started initiative of the European Justice and Home Affairs Council.

Japan

In November 2007, Japan began photographing and taking digital fingerprints of all those entering the country, residents as well as tourists and visiting businessmen. The Japanese government said the measures are simply to keep terrorists out. Yet terrorism in Japan has only ever been home-grown, most recently in 1995, when a sarin gas attack by a religious cult killed 12 in Tokyo’s subway. As it is, frequent travellers, Japanese as well as foreign residents, may save time by pre-registering to use an unmanned automatic gate at airports that takes photographs and fingerprints.

United States

The Japanese system mirrors the US-VISIT program, which was launched following the 11 Sept 2001 terrorist attacks. Travellers to the US require a machine readable, RFID-embedded biometric visa containing their fingerprints and digital photographs. The program has recorded images and fingerprints of nearly 100 million people entering the country since its launch in 2004. The scheme was supposed to automate the processing of visitors entering and exiting the country and to ensure that the millions of passengers entering the United States each year are the same people who obtained visas at US consulates abroad. US officials now take prints of all 10 fingers because they are more reliable than just two. A DHS spokesman said more fingerprints give the authorities more opportunities to check them against a watch-list of 2.5 million prints that includes known and suspected terrorists, sexual predators and people wanted on criminal and immigration charges.

Also recently, the US State department said it would offer a passport card containing an embedded RFID chip to Americans who travel frequently between the United States, Canada, Mexico or the Caribbean. The cards can be read wirelessly, offering convenience to travellers but raising security and privacy concerns about the possibility of data being intercepted. The goal of the passport card, an alternative to the traditional passport, is to reduce the wait at land and sea border checkpoints and to check travellers against watch-lists while they wait. The $45 card will be optional and cannot be used for air travel. Travellers can opt for a more secure e-passport that costs $97. Privacy and security experts said the new, less expensive passport cards can readout over longer distances and are thus more vulnerable to interception and cloning.

China – a step further

In August 2007, residents of Shenzhen, a city of 12.4 million people, became a test bed for new residency cards fitted with powerful computer chips. Data on the chip includes not just the citizen’s name and address but also their work history, educational background, religion, ethnicity, police record, medical insurance status and landlord’s phone number. Even personal reproductive history is included for enforcement of China’s controversial “one child” policy. Plans are being studied to add credit histories, subway travel payments and small purchases charged to the card.

4.2.2 Challenges

The introduction of biometric documents and electronic identities poses many challenges to privacy and the protection of personal data and, consequently, has generated lots of controversy.

---

Identity cards and passports can be forged

The new biometric ID cards and passports are more difficult to forge than those that they replace – difficult, but not impossible, as security researchers have demonstrated with a software tool that makes it easy to copy and modify identification data encoded onto the computer chips embedded in biometric passports issued by dozens of other countries. The data encoded on the e-passport chips is signed with cryptographic keys held by the issuing country, which allows the issuing country to tell if a citizen has altered the data on the device. The problem is that only 10 of the 45 countries that issue e-passports have agreed to share the public keys needed to test the integrity of the data on one another’s passport chips and, of those, only five countries are actively sharing the data. As a result, someone who has changed his name or swapped a new photo on an e-passport chip can simply sign the information using his own personal cryptographic key, and relatively few countries would be able to detect the manipulation.

Various measures have been adopted to help protect the data carried on the chips embedded in the cards and passports. One such measure is that each chip has a unique identifying number linked to information in a secure government database but not to names, social security numbers or other personal information.

The snag is that, as yet, there is no central biometric database of European citizens, which limits the utility of the ID cards and passports at least, for officialdom. The VIS (see above), however, will change that.

Fraudsters could acquire multiple cards and identities

Critics have charged that the system would not prevent fraudsters from acquiring multiple identity cards or electronic identities under different names. To obtain a biometric identity card or passport, one must first prove identity using existing (“breeder”) documentation, which could be forged.

Biometrics are not perfect

Biometrics are not 100 per cent accurate. Even if we all have unique irises, fingerprints or whatever, matching those scanned against a central database can result in false negatives (they let the suspect slip through) and false positives (they identify someone as the suspect when in fact they are not). Some biometrics are not very good. Even fingerprints, the most widely used biometric, can be unreliable. Manual work wears down builders’ fingerprints and surgeons

---

402 Brandon Mayfield, a lawyer in Oregon, was arrested in 2004 after the FBI definitively and mistakenly concluded that his fingerprints matched one taken from a plastic bag containing detonator caps found at the scene of the bombings in Madrid that year. In addition to the embarrassment and negative publicity, the FBI’s error cost the US government $2 million to settle the lawsuit filed by Mayfield. See Liptak, Adam, “Adding to Security but Multiplying the Fears”, The New York Times, 26 Feb 2007.
face similar problems because of all the hand-washing they do. Cuts on the fingers can also affect the ability to accurately match fingerprints with those stored on a database. The fingerprints of young children and the elderly are not regarded as reliable. And, of course, not everyone has fingerprints – some people have been disabled by missing hands or arms. The reliability of iris scans is affected by environmental variables such as lighting conditions and body temperature, so much so that a system can fail to match two scans of the same iris taken under different conditions. Contact lenses can also fool iris scans. With a database of every man, woman and school-age child of say 60 million records, and 99 per cent reliability, this would still mean at least 600,000 false matches. And, as with fingerprints, not everyone has eyes.

**Skimming**

Some critics have raised concerns about “skimming” data from RFID-embedded passports where some evil-doer could use an RFID reader to capture data from the new passports. US government tests confirmed privacy advocates’ suspicions that the electronic passport might be vulnerable to skimming from a distance greater than officials had previously said, meaning a matter of three feet or so instead of inches. To prevent that, the special electronic passport readers used by customs officials in the United States and their counterparts around the world would use data printed on the new passport to effectively unlock the chip before it would transmit the personal electronic information it holds. The personal data flowing to the passport reader would also be encrypted, so that someone trying to use an unauthorised reader in the area could not intercept and decipher the identity of the passport holder. Furthermore new test results show that it is impossible to move the necessary equipment and operate discretely at the same time. In consequence, this means that it can not be excluded that persons try to “skim” such documents, but the chances of this being successful and undetected are low.

---


[404](http://www.edps.europa.eu/EDPSWEB/edps/lang/en/pid/45) See the recent Opinion of the European Data Protection Supervisor (EDPS), in which he states, “The imperfections of fingerprint systems do not only concern younger children but also the elderly. It has indeed been demonstrated that accuracy and usability of fingerprints decrease as people grow older… Following the reasoning for the age limit of children, the EDPS recommends that an age limit for elderly which can be based on similar experiences already in place (US Visit has a limit of 79 years) is introduced as an additional exemption.” European Data Protection Supervisor (EDPS), Opinion on the proposal for a Regulation of the European Parliament and of the Council amending Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States, Brussels, 26 Mar 2008. http://www.edps.europa.eu/EDPSWEB/edps/lang/en/pid/45


Insecurity of central databases

One reason for the Scandinavian advancement in e-government is the centralised databases provided by the system of national identification numbers. Although there are no problems known in Denmark or Sweden concerning data losses or misuse, there is a lot of resistance against the implementation of such databases in other countries. Such fears have been echoed by the European Data Protection Supervisor who has noted that several Member States have envisaged the implementation of a central database for storing biometric passport data. “This option presents additional risks regarding the protection of personal data, such as the development of further purposes not foreseen in the regulation, or even fishing expeditions into the database which will be difficult to mitigate.”

Function creep

Function or mission creep (or repurposing) occurs when data are used for a purpose different from that specified when the data were originally collected. There are fears that the personal data, including biometrics, captured for identity cards, visas and passports will be used for different purposes. The European Data Protection Supervisor has for example expressed concern about passenger name records (PNR) being used this way as well as the transfer of such data to third countries.

Even the above-mentioned STORK project, sponsored by the Commission, Member States and private sector, suggests multiple uses of databases, as it is intended to allow easy access to social security, medical prescriptions and pension payments.

Procedural lacunae

As the legal standing of biometric ID cards has been called into question by numerous stakeholders, it is essential that such schemes are well rooted in law and stakeholder consultation. Otherwise, government (and Commission) officials can expect comments like that of the EDPS who fractiously complained that he was not consulted about the Commission’s proposal of 18 Oct 2007 to amend Regulation (EC) 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States. He pointed out that the Commission is expected to consult the EDPS when it adopts a legislative proposal relating to the protection of individuals’ rights and freedoms with regard to the processing of personal data. He also noted that the Commission did not conduct an impact assessment of its proposal, and thus it was unclear how the Commission could

---

408 See the Article 29 Working Party’s Opinion no. 3/2005 of 30 September 2005 (WP 112)
409 See the comment of the EDPS: “The main purpose of a passport is to facilitate the travel of European citizens”. EDPS, Opinion of 26 Mar 2008, op. cit.
properly evaluate the necessity and proportionality of the proposal in relation to data protection issues.\textsuperscript{413}

**Harmonising “breeder” documents**

Issuing passports is a responsibility of the Member States under each country’s national law, which requires the presentation of various documents, such as a birth certificate, citizenship certificate, family book, parental authorisation, driving licence, utility bill, etc. These documents are sometimes called “breeder” documents, as passports may stem from them.

The EDPS has noted that the way “breeder” documents are produced in the Member States and the documents required for delivering a passport show a great diversity of situations and procedures, which are bound to decrease the quality of data in passports and even to foster the risk of identity theft. With fewer security features, “breeder” documents are more likely to be subjected to forgery and counterfeiting than a biometric passport.

Although the EDPS welcomed the objective of the Commission to enhance passport security measures, he stressed that the passport is only one link in a security chain starting from the “breeder” documents and ending at the border check points, and that this chain will only be as secure as its weakest link. He therefore recommended that the Commission propose additional measures for harmonising the way in which “breeder” documents are produced and which of them are required for a passport.\textsuperscript{414}

4.2.3 **Final remarks**

Obviously biometric documents and electronic identities can create new or fortify existing problems in privacy and trust, but there are also good examples for the use of such systems without problems. The combination of both, i.e., electronic identities based on biometric documents, seems to be highly problematic, although the argument for this is often the higher security level of such systems. This illustrates also the problem of dealing with this question within this report, because some of the challenges are connected to problems of “Third Pillar” activities at EU level or even at Member State level, which are beyond the scope of this report.

4.3 **SMART TRANSPORTATION SYSTEMS**

In the case of smart transportation systems, two different scenarios have to be considered – first, private transport and, second, public transport. As each has different requirements and challenges, we will look at each separately.

4.3.1 **Private transport**

Many cities and several countries have started to use ICT to closely monitor and control traffic by technology-based toll systems. The systems were introduced to ease traffic congestion and/or improve road safety, but such systems are fulfilling other needs too, e.g., in catching offenders and preventing crime. These systems are not confined to vehicle traffic: the exchange of passenger name records (PNRs) offers a similar means of tracking air travel.

\textsuperscript{413} EDPS, Opinion of 26 Mar 2008, op. cit.
\textsuperscript{414} EDPS, Opinion of 26 Mar 2008, op. cit.
Most recently, rail traffic has come under similar scrutiny, but results from a proof-of-practice test in Germany showed the limitations (as described above in section 2.1.2 Identification technologies).\textsuperscript{415} Somewhat in contrast to car traffic control systems, the reason for introducing PNR systems was the prevention of terrorism. Although developments in all cases – such as the negotiations between the EU and the US about flight passengers’ data, the use of information collected by toll systems and plate recognition for law enforcement in Germany and other countries – have been intensively discussed in public, the discussions have followed different patterns. For instance, after the events of 11 Sept 2001, the topic of passenger data was not much discussed, at least, not compared to the use of plate recognition which was discussed at length from the beginning. These traffic monitoring systems, whether by road, rail or air, offer good opportunities for function creep, for using data collected for one purpose for other purposes. Although obviously not their intention, they also prey on citizens’ fears of a Big Brother society. As a result of these fears, stimulated by media attention and the ensuing controversy, numerous regulations were implemented along with high court judgements, as in Germany.\textsuperscript{416} A less considered challenge to privacy results from the fact that most of these traffic monitoring systems are driven as public-private partnerships. This possibly opens the threat of creating travel patterns by private companies.

Starting in early 2009, T-Systems Traffic, a subsidiary of Deutsche Telekom AG, will provide the TMCplus (Traffic Message Channel Plus) navigation service. TMC is a technology for delivering traffic and travel information to drivers over radio broadcasts. Navigation systems can make use of this information to calculate alternative routes. TMCplus makes use of the so-called “floating-phone-data” (FPD or Net-FCD) which is generated when a mobile phone is changing from one cell to another. These data, which network operators normally use for network management, can also be used to derive time-space trajectories of car travellers.\textsuperscript{417} Data protection authorities were concerned about the secondary use of mobile phone data for these purposes, especially since T-Systems Traffic used to be a subsidiary of T-Mobile before becoming a separate company within Deutsche Telekom. Mobile phone companies claim, however, that they are allowed to use FPD because “the data is necessary for network management and therefore we own it”.\textsuperscript{418} The network operators assure that before the data are used for calculating traffic data, individual phone numbers will be replaced by random numbers.\textsuperscript{419}

A more recent development, which will pose new challenges to privacy and trust, is the development of vehicle safety communication technologies, which is one of the objectives of the EC’s Seventh Framework Programme. The major aim of vehicle communication is that traffic should be accident-free, efficient, adaptive, cleaner and comfortable. Such technologies enable communications directly between vehicles and/or with road infrastructure systems and/or with law enforcement or other authorities. They may use autonomous, self-organising, wireless communications networks which can also be connected with in-car sensor

\textsuperscript{416} BVerfG, 1 BvR 2074/05 vom 11.3.2008, Absatz-Nr. (1 - 185). http://www.bverfg.de/entscheidungen/rs20080311_1bvr207405.html
\textsuperscript{419} Asendorpf, Dirk, “Nützliche Verräter”, Die Zeit, 6 Nov 2008.
Among the first deployments of such vehicle communication systems are parking assistance systems. While traffic monitoring systems enabling licence plate recognition require an active engagement of the state authorities, for example, by scanning and verifying plates, vehicle safety communication is based on an active transmitter, which broadcasts information into the environment.

Such systems will make a big difference in the accessibility of personal data because public authorities will only need to intercept this communication. They also offer the possibility that unauthorised third parties may gain and use traffic information if the security standards of the communications protocols are inadequate. Therefore, there is not only the challenge of secondary use of data by state authorities, there is also a possibility for fraud, misuse or manipulation by third parties, especially where the systems are operated by public-private partnerships.

That is why car-to-car and car-to-infrastructure communications systems raise questions about whether one’s private car should be regarded as a private or a public place. Sociologically, the private car is essentially a private place used by their owners like an extension of their private homes. On the other hand, the car is moving through the public sphere where different privacy rules apply. Thus, one crucial question is how hybrid spaces like cars should be treated with respect to privacy.

### 4.3.2 Public transport

Around the world, smart cards based on RFID technology are becoming more common in transport. More than 80 per cent of the mega cities worldwide are already using smart cards and smart tickets in public transportation (Tokyo: 20 million chip cards; Mexico City, New York City, Seoul: over 10 million each). The market for these cards is divided into two segments: the low- and mid-range cards using normal contactless RFID-cards and high-end multi-application cards including payment functions using microcontrollers. In addition to approximately 150 million chip cards worldwide, there are as many paper tickets with RFID chips. Most of cities are using one of the four proprietary systems: ASK’s Calypso® (Mexico City, Milan, Athens, Paris, etc.), Philips and Infineon’s Mifare® (Cairo, Taipei, Seoul, Moscow, London, etc.), Sony’s FeliCa® (Hong Kong, Bangkok, Singapore, Shenzhen, etc.) and CUBIC’s GO Card® (Guangzhou, Chicago, Rotterdam, etc.). Because in most of the cities multiple companies operate public transport, these smart cards and tickets also form the basis of clearance among these companies.

Contactless ticketing schemes have many advantages. Transport for London (TfL) has estimated that after the introduction of its Oyster card, 1 million fewer transactions per week are made at ticket offices and that there is a 30 per cent improvement in the speed of passengers passing through the ticket gates. TfL also states that it is more difficult to copy Oyster cards than the magnetic stripe cards and, as each card contains a unique ID number, it can be immediately cancelled if the card is reported lost or stolen. In June 2008, however,
scientists at a Dutch university hacked and cloned Mifare smartcards\(^\text{423}\) (used in the Oyster cards and the Dutch OV-chipkaart\(^\text{424}\)). Such a security flaw can pose some serious challenges to privacy as well.\(^\text{425}\) The possibility of “cloning” the RFID chips allows hackers to use another person’s identity. This challenge could be even more serious if additional personal information is stored on the card, e.g., on a multi-application card.

Even a properly working electronic ticketing scheme raises privacy concerns. As long as the RFID system merely functions as a payment system, identity management is basically a matter of distinguishing between people who have paid or those who haven’t – and, in some, differentiating between one-off tickets and discounted tickets (such as seasonal tickets). However, these cards open up many opportunities for the operator of the system to monitor travelling behaviour. In a contactless ticketing scheme, a link to the user is established through a unique code etched onto the RFID chip embedded in the travel card, which is scanned on every entry or exit. Depending on the actual implementation, this link can be anonymous, but provides information for building movement profiles, which is valuable for marketing purposes.

In many cases, transport companies favour personalised cards because they want to use the data generated by travellers for marketing purposes and for providing new services (such as a credit card function) to the customer. Though data protection authorities have expressed their concerns (as in the case of the Dutch Railways card scheme), there are more reasons for introducing personalised cards. For now, they are cheaper than anonymous cards, and government authorities see opportunities to use this information for law-enforcement purposes.

The Dutch case also shows what concerns citizens. A technology assessment (TA) report for the European Parliament on RFID and Identity Management indicates that many citizens are concerned that governments are gathering more information about them and their whereabouts. Some fear the police soon will get access to all travel data, or data will be used for all sorts of commercial purposes such as advertisements. Others worry about the security of the travel data and explicitly criticise the lack of choice: when using the public transport regularly – and therefore using a discount card or a subscription – they cannot travel anonymously.\(^\text{426}\)

4.3.3 Challenges

Although data collection in private and public transport systems differs from the technological point of view, the challenges that arise are broadly similar. In both cases, the most significant challenges are the possibility to generate detailed individual movement profiles and the risk of misusing payment systems. The creation of movement profiles is possible through various methods including electronic toll systems, optical tracking using car plate recognition, etc.

Since many smart transportation systems are developed and operated by private-public partnerships, movement profiles offer the opportunity for secondary use by enterprises for

---


\(^\text{426}\) ETAG (European Technology Assessment Group), Christian van’t Hof, op. cit., p. 15.
marketing purposes and government authorities mainly for law enforcement.

Moreover smart transportation systems can be used for criminal activities when the security mechanisms are weak and allow identity theft on a larger scale. This is especially true in the case of future intelligent vehicles that will store a lot of information about its owner. Since there is a trend towards considering the car as a node in the "evernet", the upcoming super-infrastructure going beyond even the vision of the Internet of things, it could become the target of hackers and attackers.

4.4 E-DEMOCRACY

The last example within this field is e-democracy. In the beginning of this chapter, we remarked that according to our understanding, e-democracy is not part of e-government, because, in e-government, citizens are mostly the object of administrative and governmental actions, whereas this situation is reversed in e-democracy. Here the citizens acts in the process of public opinion and voting, which legitimates government and administration. Nevertheless, there are also a series of questions concerning privacy and trust, that arise in connection with the administration of electronic voting procedures. Even though the main challenges do not differ between e-democracy and e-government, there are some important differences between both fields concerning the role of citizens.

Most experts regard building the support of public opinion by means of ICT as e-democracy. This covers a broad range of activities and because of this, the use of terms such as e-democracy or e-voting is inconsistent. Additionally, the topic has raised a lot of public interest as a result of the recent and past US presidential election campaigns where candidates have made significant use of the Internet, supported by public discussions by bloggers, the use of YouTube as a broadcast platform and fund-raising via websites. In the following section, we look at ICT support for the voting process itself (e-voting). From a privacy point of view, the fundamental condition of the secret, general, equal and free vote creates the greatest privacy challenge.

E-voting

E-voting is usually regarded as voting by electronic means. In some cases, experts restrict this definition even more, when they define it as electronic voting via a private or public PC, mobile or comparable device. Voting machines would be excluded from this definition. Such an exclusion is, however, somewhat irrelevant, at least in the context of challenges to privacy and trust. Voting machines and electronic voting both raise similar questions with regard to their security and confidentiality (privacy) and their usability (trust). Even so, we will not give an overview of the discussion on voting machines, except to say that in several countries,
including the US, Netherlands, France and Germany, their use is, at least partly, allowed and they are the subject of various reviews, reports, legislative regulations and high-court judgments,\textsuperscript{431} which have been accompanied by a massive public debate.

While voting machines have attracted a lot of attention, especially because of their role in the US presidential elections in 2000 and 2004, the discussion about electronic voting seems only of interest to experts. Nevertheless, the challenges to privacy are fundamental to the voting practices in a democracy\textsuperscript{432} and, consequently, of relevance to all stakeholders.

**Challenges**

Experts have raised a series of questions and concerns.

- One major issue is the possible technical procedures, which must allow for a secret vote by each voter. Various cryptographic solutions have been proposed, but they are doubts about their security in practical applications. Ubiquitous computing will make new demands on the technical procedures.\textsuperscript{433}

- Another topic, closely related to the technical procedures, is the speed of voting. Some experts argue that the act of voting, including actually going to the voting booth and making a cross against the chosen candidate, offers the possibility for further reflection which, in their eyes, would not happen in the case of e-voting.

- Similarly, some argue that the transfer of voting from a public place to private homes would harm the feeling of citizenship, because the ritual of voting in the voting booth at a public place can create a feeling of belonging to an active community of citizens.

- A fourth, rarely discussed topic is the extent to which online voting would have an impact on generality—i.e., would e-voting discriminate against people on the wrong side of the digital divide, without the requisite knowledge and/or equipment? In addition to these questions, national law may stand against online voting. Even if all these issues were resolved satisfactorily, no one can guarantee secret and free voting in the case of e-voting. It would, of course, be impossible to see if people were alone when they voted or under pressure to vote in a certain way when they sat in front of a computer screen.\textsuperscript{434} This last issue is the most serious, indeed, it may be a show-stopper.

---


\textsuperscript{432} See also Buchstein, Hubertus, “Präsenzwahl, Briefwahl, Onlinewahl und der Grundsatz der geheimen Stimmabgabe”, Zeitschrift für Parlamentsfragen, Vol. 31, No. 4, 2000, pp. 886-902.


\textsuperscript{434} Buchstein, Hubertus, op. cit.
5 INTERNATIONAL TRANSFERS OF PERSONAL DATA

No matter what privacy principles and legislation we have in Europe, we must recognise that we live in a globalised, interconnected world where much of the economy is fuelled by personal data\(^{435}\), which flows easily from one country to another, often beyond the reach of European regulatory power.

Increased globalisation means more businesses want to transfer such data across borders, but data protection legislation says they should not do so without regulatory approval. The snag for business is that it must deal with many different regulatory approaches and requirements over data protection around the world. These differences affect European industry operating globally as much as it does non-EU based industry with offices in Europe.

In addition to transfers of personal data for business purposes, governments have interests in the exchange of personal data such as for combating crime and terrorism, but they too have encountered difficulties in effective and legitimate ways of doing so. Individuals travelling from country to country may also find customs authorities rifling through personal data on their laptops and mobile phones.\(^{436}\)

The problems arising from the transfer of personal data across borders are complicated by nominally competing values – privacy aims to protect personal data, while personal data fuels business – and differing regulatory regimes.

This section reviews some recent cases involving transfers of personal data from the EU to third countries, highlights some key issues, summarises what has been done so far to deal with the challenges posed by international transfers of personal data, current initiatives and other needed responses. The complexities of international transfers of personal data remain a potent and not adequately resolved issue, as reflected in its continuing to be a hot topic in various meetings of data protection authorities and other privacy experts.

5.1 TRANSFERS VIA THE INTERNET

When signing on to non-EU websites, Europeans are agreeing to export of their data whether they know it or not. The Commission has admitted that the Internet, and new possibilities for data subjects to interact and to access services provided in third countries raise questions on the rules for determining the applicable national law or for transfers of data to third countries, issues to which case law has given only a partial answer.\(^{437}\)

\(^{435}\) A May 2000 US Federal Trade Commission survey of 426 websites (including 91 of the 100 busiest and 335 randomly selected) found that the websites collected a vast amount of personal information from and about consumers. Almost all sites (between 97 and 99 per cent) collected an e-mail address or some other type of personal identifying information. Most sites surveyed were capable of creating personal profiles of online consumers by tying any demographic, interest, purchasing behaviour or surfing behaviour information they collect to personal identifying information. Bureau of Consumer Protection, Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress, Federal Trade Commission, Washington, DC, May 2000, pp. 9-10. http://www.ftc.gov/reports/privacy2000/privacy2000.pdf.


Does European data protection law protect European users of websites based in the US or other countries outside the Union? According to the Article 29 Working Party, it does. The Working Party discussed the issue of the international application of EU data protection law to personal data processing on the Internet by non-EU based websites in a working document in 2002, the gist of which is paraphrased in the following paragraphs.438

The Working Party said the Directive applies even if the data controller is not established on Community territory, but decides to process personal data for specific purposes and makes use of equipment, automated or otherwise, situated on the territory of a Member State. Recital 20 of the Directive explains that “the fact that the processing is carried out by a person established in a third country must not stand in the way of the protection of individuals”.439

The Working Party gives some practical examples, one of which is where the controller decides to collect personal data by means of a cookie placed on a user’s computer, while a copy might be kept by the website or a third party. In the case of further communication, the information stored in the cookie (and therefore on the user’s computer) is accessed by the website in order to identify this computer to the controller. According to the Working Party, the user’s computer can be viewed as equipment in the sense of Article 4.1(c) of the Directive. It is located on the territory of a Member State. The controller decides to use this equipment for the purpose of processing personal data and several technical operations take place without the control of the data subject.

The Working Party said the user should be informed when a cookie is intended to be received, stored or sent by Internet software, which information is intended to be stored in the cookie and for what purpose as well as the period of validity of the cookie. The user should be given the option to accept or reject the sending or storage of a cookie and options about which pieces of information should be kept or removed from a cookie. That’s what should happen, but in reality, it rarely does.

According to Article 18.1, the controller or his representative must notify the data protection authority before carrying out any processing. Member States may provide a simplification of or exemption from notification for processing operations that are unlikely to affect adversely the rights and freedoms of the data subjects.

The snag is enforcing these provisions. The difficulty of doing so was exemplified by an October 2008 press release in which the Article 29 Working Party said “Google refuses for the moment to submit to the European data protection law.”440 The press release referred to the Working Party’s opinion on search engines, published in April 2008, in which it reaffirmed the applicability of European data protection law, recommended a maximum retention period of six months and said that Web users must be able to provide consent to the exploitation of their data in particular for profiling purposes. It noted Google was failing to meet the Working Party’s expectations.

438 Article 29 Data Protection Working Party, Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites, 5035/01/EN/Final, WP 56, Adopted on 30 May 2002.

439 The Working Party noted that Article XIV of the GATS allows countries to lay down exemptions from the free trade rules in order to protect individuals with regard to their right to privacy and data protection and to enforce this law.


5.2 **LAPTOPS CAN BE INSPECTED**

Personal data can be physically transported across borders when travellers carrying their mobile phones or laptop computers go from country to country. Customs officials can inspect their baggage, of course, but probably most people have yet to realise that they can also “inspect” our electronic toys, including the files therein.

Critics have argued that rifling through our laptops without a warrant or even a reasonable suspicion of criminal activity is an invasion of privacy and open to all sorts of abuse. Among other things, some have concerns that inspecting laptops at borders could compromise corporate secrets, a lawyer’s confidential documents, a journalist’s notes from a protected source, or personal financial and medical information.

So far, there is virtually no information about how often such searches or seizures take place, who gets selected, what the government does with any copied data, who has access to such data, what safeguards are in place, and how the data are stored and eventually destroyed. Information that is protected within a country may not enjoy the same protection when it is transported across borders.

In the United States, a Federal District Court initially rejected the government’s argument that a search of a laptop is no different than rifling through luggage during arrivals inspection. The court suppressed the warrant-less and suspicion-less laptop searches as unreasonable. However, in April 2008, the 9th US Circuit Court of Appeals ruled that customs officials may indeed inspect laptops and other personal electronic-storage devices without suspicion.

Critics argue that laptops aren’t the same as luggage because laptops typically carry far more information and the contents may be confidential or highly personal. They are an extension of a person’s professional and personal identity.

The Electronic Frontier Foundation filed a lawsuit in 2008 to determine the scope of such searches, saying that Department of Homeland Security (DHS) had not responded to previous requests for records.

US Senator Russell Feingold, who convened a Senate subcommittee hearing in June 2008 on the subject of “Laptop Searches and Other Violations of Privacy Faced by Americans Returning from Overseas Travel”, is considering legislation to require reasonable suspicion for border electronics searches; to let the public know what rules are in place for copied data; and to ensure that racial, religious or ethnic profiling doesn’t occur.

The US is not the only country where travellers’ laptops may be searched. Canada also engages in the activity. *The Globe and Mail*, which bills itself as Canada’s national newspaper, commented in an editorial that “It is disturbing that this intrusion can occur even without reasonable suspicion” and then argued that travellers should be made aware of the possible extent of border searches before they travel, and customs and border agencies have a responsibility to make their policies clear and accessible.
5.3 CHALLENGES POSED BY INTERNATIONAL TRANSFERS OF PERSONAL DATA

Most people don’t know who has their data, what they are doing with their data, how they can check the accuracy of their data.

International transfers of personal data raise jurisdictional, compliance and enforcement issues, e.g., in which jurisdiction should a European seek redress for any wrongful use of his data. How can I be sure my data are not being abused and how can I obtain redress if they are?

There are administrative issues, e.g., how easy or possible is it for a European to get access to his data, to correct them if there are errors, to find out to whom his data might have been further transferred and for what purpose, and to seek redress if he feels he has been wronged.

Generally, there is a lack of accountability once personal data are transferred outside Europe to a third country. A citizen of the EU lacks power to enforce her rights in a non-EU country, especially when the third country does not have an adequate data protection regime.

There are also procedural inequities and challenges. Heretofore, most stakeholders have had scant opportunity to provide any input into the formulation of arrangements for the transborder transfer of personal data. Given the criticism that such arrangements have suffered, policy-makers may adopted new, more consultative procedures in the future, but so far that remains to be seen.

5.4 WHAT HAS BEEN DONE SO FAR TO DEAL WITH THE CHALLENGES

The problems and challenges posed by the international transfer of personal data have been apparent for decades. One of the early and best-known attempts to deal with the matter on an international level was undertaken by the OECD. The OECD initiative and those of others are briefly described in the following paragraphs.

5.4.1 OECD initiatives

The OECD recognised the problems arising from the transborder flows of personal data three decades ago, long before the World Wide Web was even created. On 23 September 1980, the OECD Council adopted a Recommendation concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data.\footnote{Organization for Economic Co-operation and Development (OECD), Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, OECD, Paris, 23 Sept 1980. http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1,00.html}

The OECD guidelines recognised that transborder flows of personal data were creating new forms of relationships among countries and required the development of compatible rules and practices. It said that transborder flows of personal data contribute to economic and social development. While it recommended that countries reflect in their domestic legislation the principles concerning the protection of privacy and individual liberties as set out in the guidelines, it also recommended that Member countries “remove or avoid creating, in the name of privacy protection, unjustified obstacles to transborder flows of personal data”. However, it goes on to say that “A Member country should refrain from restricting
The guidelines thus deal with two nominally competing values, protecting privacy and the free flow of personal data across borders. Priscilla Regan has pointed out that, in content, tone and enforcement, the guidelines represented a compromise between the interests of the United States in maintaining the free flow of information and those of the European countries in achieving consistent regulations protecting personal information.\(^{442}\)

The explanatory memorandum which is a part of the Guidelines says that the problems of developing safeguards for the individual in respect of the handling of personal data cannot be solved exclusively at the national level and that the regulation of the processing of personal data should be considered in an international context.

The guidelines set out a number of, by now, familiar principles relating to collection of data with the consent of the individual, purpose specification, use limitation, security safeguards, openness\(^{443}\) and so on. The guidelines remain in force, which can be taken as a sign of their robustness and continuing relevance. Indeed, they have inspired a lot of the data protection and privacy legislation since their formulation.

Nevertheless, the world has (obviously) moved on since 1980; new technologies and new complexities in the transfer of personal data across borders have arisen. The OECD has continued to study the issue.

The OECD released a Report on the Cross-border Enforcement of Privacy Laws in October 2006. The report looks at the law enforcement authorities and mechanisms that have been established with a particular focus on how they operate in the cross-border context. It describes existing arrangements to address the challenges and identifies a number of issues that require further consideration.

To further explore the cross-border challenges, the OECD, together with Canadian Privacy Commissioner Jennifer Stoddart, organised a Roundtable on Privacy Law Enforcement Cooperation in London in November 2006. Another OECD roundtable followed in March 2007.

On 12 June 2007, the OECD Council adopted a new Recommendation setting forth a framework for co-operation in the enforcement of privacy laws. The framework reflects a commitment by governments to improve their domestic frameworks for privacy law enforcement to better enable their authorities to co-operate with foreign authorities, as well as to provide mutual assistance to one another in the enforcement of privacy laws.

One part of the Recommendation calls for a consultation between privacy authorities and privacy professionals on how best to resolve privacy complaints.


\(^{443}\) The Guidelines say that “Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.” Nevertheless, most individuals confront a real difficulty in knowing who has their data and what they are doing with them.
The OECD story has not stopped there as, in May 2008, it held yet another roundtable on the issue.\footnote{http://www.oecd.org/document/25/0,3343,en_2649_34255_37571993_1_1_1_1,00.html}

5.4.2 Council of Europe

The right to privacy is specifically mentioned in the Council of Europe’s 1950 Convention for the Protection of Human Rights and Fundamental Freedoms.\footnote{Article 8.1 says “Everyone has the right to respect for his private and family life, his home and his correspondence.” The right to privacy is not, however, absolute and is balanced against other values. Article 8.2 of the Convention says “There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. http://conventions.coe.int/Treaty/Commun/QueVoullezVous.asp?NT=005&CM=8&DF=12/9/2008&CL=ENG\footnote{http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm} and Regulation (EC) No. 45/2001. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001R0045:EN:HTML\footnote{Regan, Priscilla M., “Safe Harbors or Free Frontiers? Privacy and Transborder Data Flows”, Journal of Social Issues, Vol. 59, No. 2, 2003, pp. 263-282 [p. 269].}\footnote{Council of Europe, Convention for the protection of individuals with regard to automatic processing of personal data, European Treaty Series, no. 108 of 28 January 1981. http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm}\footnote{Council of Europe, Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows (ETS No. 181), 8 Nov 2001. http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/} The Council of Europe debated the issue of privacy and transborder transfers as long as 1968, when it concluded that national and international law was not adequately protecting privacy. In 1974, the Council adopted non-binding recommendations that information should be accurate, timely and relevant; confidentiality and security should be protected; individuals should have rights of access, notice, consent and correction. It also drafted an international treaty on data protection to clarify the right of privacy in the European Convention on Human Rights. This “Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data” was binding on the countries that signed it and required that national laws be consistent with it. The United States did not sign the Convention.\footnote{Regan, Priscilla M., “Safe Harbors or Free Frontiers? Privacy and Transborder Data Flows”, Journal of Social Issues, Vol. 59, No. 2, 2003, pp. 263-282 [p. 269].}

In 1981, a few months after publication of the OECD Guidelines, the Council of Europe adopted the Convention for the protection of individuals with regard to automatic processing of personal data.\footnote{Regan, Priscilla M., “Safe Harbors or Free Frontiers? Privacy and Transborder Data Flows”, Journal of Social Issues, Vol. 59, No. 2, 2003, pp. 263-282 [p. 269].} It was the first binding convention on data protection, and the only binding international legal instrument in the field. Its aim is to protect the individual against abuses that may accompany the collection and processing of personal data. The Convention also contains provisions on cross-border flows of personal data. The Convention has been amended by additional protocols, one of which deals with transborder data flows. The Protocol concerns the provision for supervisory authorities responsible for ensuring compliance with the measures in domestic law giving effect to the Convention. Furthermore, like the OECD guidelines, it provides that transfer of data to countries not subject to the Convention shall only be possible if an adequate level of protection is assured.

5.4.3 Data Protection Directive (95/46/EC)

Richard Thomas, the UK Information Commissioner, told a conference in Cambridge in July 2008 that Europe's data protection laws are no longer fit for purpose. “European data protection law is increasingly seen as out of date, bureaucratic and excessively prescriptive. It is showing its age and is failing to meet new challenges to privacy, such as the transfer of personal details across international borders and the huge growth in personal information...
Transfers of personal details across international borders are governed by Articles 25 and 26 of the Data Protection Directive (95/46/EC). Article 25, which lays down the principles, says transfers of personal data to third countries can take place only if the third country ensures an adequate level of protection. So far, the European Commission has recognised only five countries as providing an adequate level of protection. Some commentators have said that Article 25 has proved “a serious headache for multi-national companies”, operating inside and outside the EEA, which often need to transfer employee or client personal data among themselves.

Article 26 lists certain exceptions (derogations) to Article 25, so that personal data can be transferred legitimately from Europe to third countries, such as the United States. These derogations include the following:

- Data can be transferred if “the data subject has given his consent unambiguously to the proposed transfer”.  
- A Member State may authorise transfers to a third country which does not have legislation comparable to the Data Protection Directive where the data controller offers “adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals”. These safeguards may be provided in appropriate contractual clauses.

Companies may obtain approval from data protection authorities for data transfers by means of contractual arrangements that comply with the Directive’s provisions. The Article 29 Working Party has developed model contracts for this purpose. Companies can also use standard contractual clauses (SCCs) approved by the Commission. These are essentially contractual arrangements between a data exporter based inside the EEA and a data importer based outside the EEA, whereby both parties undertake not to infringe the Directive. To facilitate the use of contractual clauses, the European Commission has issued three decisions on standard contractual clauses.

The Commission adopted a decision recognising an additional set of contractual clauses to provide adequate safeguards for transfers of data to controllers in third countries. These clauses were proposed by a group of representative business associations, including the

---

449 ICO awarded a contract to Rand Europe to make recommendations on modernising the European Data Protection Directive. Its findings are expected in the first half of 2009. In 2007, the Commission said that it regards the Data Protection Directive as technologically neutral and does not envisage submitting any legislative proposal to amend the Directive. See COM(2007) 87 final, p. 9. However, the Commission may be rethinking the matter. In 2008, the EC Directorate General Justice tendered a contract to review the adequacy of the Data Protection Directive. It was also awarded to Rand.

450 The Article 29 Working Party adopted an Opinion laying down important elements for guidance on the use of the exemptions to the principle of adequate protection in third countries.

See also http://ec.europa.eu/justice_home/fsj/privacy/modelcontracts/index_en.htm
International Chamber of Commerce. The Commission presented a first report on the implementation of the previous Commission decisions on contractual clauses in 2006.\footnote{European Commission, Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive, COM(2007) 87 final, Brussels, 7 Mar 2007.} According to the Article 29 Working Party, the standard contractual clauses 2002/16/EC have provided “a solid base” for the transfer of personal data.\footnote{Article 29 Data Protection Working Party, Opinion 3/2009 on the Draft Commission Decision on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC, 00566/09/EN, WP 161, Adopted on 5 March 2009, p. 2} However, as more companies outsource the processing of data, the call for an update of this contract has been growing louder. Some companies not only transfer their data to a processor but to “sub-processors”, but the standard contractual clauses 2002/16/EC do not provide a means to deal with such onward transfers. Hence the European Commission proposes to modify the standard contractual clauses 2002/16/EC to make a contract better equipped for current business arrangements by adopting a new Decision based on Article 26(4) of Directive 95/46/EC.

Meanwhile, the Article 29 Working Party has called upon the Commission to consider situations where data controllers and data processors in the EU outsource the processing of data to a sub-processor in a third country which does not have adequate safeguards, in particular when sensitive data are processed or in case of processing operations carrying specific risks to data subjects (i.e., biometric data, genetic data, judicial data, financial data, data on children, profiling).

One of the reasons why contractual arrangements have not proved to be popular with multinational companies, however, because they have had to agree to joint and several liability provisions. Multi-nationals has thus sought viable alternatives\footnote{Rees, Philip, and Dominic Hodgkinson, “Binding Corporate Rules: A simpler clearer vision?”\cite{Rees2007}, Computer Law & Security Report, Vol. 23, 2007, pp. 352-356.}, such as the Safe Harbour agreement and Binding Corporate Rules (BCRs), which are discussed in more detail in the following paragraphs.

**Safe Harbour Agreement**

Companies operating globally are confronted with a serious challenge in that some countries have adopted different approaches and different requirements with regard to privacy and data protection (where they have been implemented at all, of course), so the rules governing the transfer of data vary somewhat. Understandably, such companies would prefer a harmonised set of rules. While not wishing to compromise EU data protection legislation, the European Commission has been sympathetic to companies. The Safe Harbour and Binding Corporate Rules (BCRs) were devised as responses to the challenges facing companies from differing regulatory regimes.\footnote{According to Priscilla Regan, American business prevailed upon officials in the International Trade Administration (ITA) of the U.S. Department of Commerce to develop a “Safe Harbor” arrangement with officials from the EC’s Directorate General (DG) XV, the Internal Market DG. Through a “Safe Harbor,” American businesses that agreed to the arrangement would be viewed as being in compliance with the adequacy requirement of the EU Directive and would ensure that their flows of personal information were not interrupted. See Regan, Priscilla M., “Safe Harbors or Free Frontiers? Privacy and Transborder Data Flows”, Journal of Social Issues, Vol. 59, No. 2, 2003, pp. 263-282 [pp. 272-73].}
Under Article 25.6 of the Directive, the Commission can determine whether a third country ensures an adequate level of data protection. If it concludes that there is adequate protection, then personal data can flow to that third country without any further safeguard. At first, the US was deemed not to offer such protection, but after protracted negotiations, the EC and the US Federal Trade Commission (FTC) came up with the Safe Harbour Agreement under which US companies would self-certify that they met basic requirements for protecting data. If they failed to comply, they could (in theory) be penalised by the FTC for making a false declaration.

Following signature of the agreement, a study carried out for the Commission found “alarming” deficiencies. The authors of the study said the deficiencies were not necessarily the result of bad faith, since most of the reviewed US organisations seemed to have difficulties in correctly translating the Safe Harbour principles into their data-processing policies, in part because of confusion over the obligations and differing perceptions of what can be regarded as personal data protection. The authors believed that these problems could be overcome by providing better guidance on the mechanics as well as the meaning of the Safe Harbour data protection principles.

It seems somewhat problematic to know how adequately the Safe Harbour Agreement is enforced on the US side. The US Department of Commerce says, “If a relevant self-regulatory or government enforcement body finds [italics added] an organization has engaged in a persistent failure to comply with the principles, then the organization is no longer entitled to the benefits of the safe harbor. In this case, the organization must promptly notify the Department of Commerce of such facts either by email or letter. Failure to do so may be actionable under the False Statements Act (18 U.S.C. 1001).” It then goes on to say that in maintaining the list of companies that say that they comply with the Safe Harbour principles, “the Department of Commerce does not assess and makes no representations to the adequacy of any organization's privacy policy or its adherence to that policy.” Thus, the DoC does not seem to actively investigate whether a company does comply. Admittedly, it says that if it “finds an organization has engaged in persistent failure to comply”, then failure may be actionable, but it does not say how it might find whether a company is complying, e.g., it does not say it checks periodically. Elsewhere on the Commerce Department’s website, it says “enforcement of the safe harbour… will be carried out primarily by the private sector.” It seems finding failure is somewhat fortuitous. There does not seem to be any data on the Commerce Department’s website on the number of companies found to be failing to comply or that have withdrawn their self-certification or whether there have been any lapses. It seems hard to believe that all 1,500 companies that have so far self-certified have adhered to the principles without failure. There also does not appear to be any data on the number of requests

456 http://www.export.gov/safeharbor. The EC has so far recognised Switzerland, Canada, Argentina, Guernsey, Isle of Man, the US Department of Commerce's Safe Harbor Privacy Principles, and the transfer of Air Passenger Name Records to the United States. For a list of US companies, numbering about 1,500, that say they comply, see: http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list


458 http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list

any of these 1,500 companies have received from Europeans seeking their personal data or how many were supplied the data and how many were not.

Others have criticised the shortcomings of the Safe Harbour agreement, including the European Parliament, industry, civil liberties groups and privacy experts. On 5 July 2000, the European Parliament expressed its view that the remedies for individuals in the proposed Safe Harbour did not provide adequate protection. The TransAtlantic Consumer Dialogue (TACD), which represents more than 60 European and American consumer protection groups, criticised the Safe Harbour agreement, saying it would not provide adequate protection to European citizens because of its reliance on a self-regulatory system that has been unsuccessful in the United States. The TACD said, “Ultimately, companies can do what they like with personal data provided they can be said to have the consumers’ consent. The real danger here is that consent clauses can be cleverly drafted to give companies almost a free hand to process data as they wish. In practice, consumers are forced to accept the companies’ terms or otherwise lose the opportunity to do business with the company (or any other company) at all.”

Joel Reidenberg describes the Safe Harbour agreement as “unworkable for both sides” and says it “will not alleviate the issues of weak American privacy protection”. He also says that European data protection agencies have expressed “substantial opposition” to the agreement. Among other weaknesses and problems with the agreement, he says,

Safe Harbor by its terms can only apply to activities and U.S. organizations that fall within the regulatory jurisdiction of the FTC and the U.S. Department of Transportation. As a result, many companies and sectors will be ineligible for Safe Harbor, including particularly the banking, telecommunications, and employment sectors that are expressly excluded from the FTC's jurisdiction. Second, Safe Harbor will not apply to most organizations collecting data directly in Europe.

Even more serious is his contention that

Safe Harbor weakens European standards for redress of data privacy violations. Under the European Directive, victims must be able to seek legal recourse and have a damage remedy. The U.S. Department of Commerce assured the European Commission that Safe Harbor and the U.S. legal system provided remedies for individual European victims of Safe Harbor violations. The European Commission expressly relied on representations made by the U.S. Department of Commerce concerning available damages in American law. The memorandum presented by the U.S. Department of Commerce to the European Commission, however, made misleading statements of U.S. law. For example, the memorandum provides a lengthy discussion of the privacy torts and indicates that the torts would be available. The memorandum failed to note that the applicability of these tort actions to data processing and information privacy has never been established by U.S. courts and is, at present, purely theoretical... Safe Harbor is also predicated on dispute resolution through seal organizations such as TRUSTe. Yet, only one seal organization, the ESRB, proposes any direct remedy to the victim of a breach of a privacy policy, and other organizations' membership lists look like a “Who's Who” of privacy scandal-plagued companies.

---


More recently, he has described the Safe Harbour agreement as “an expedient effort to avoid confrontation between the United States and Europe” and opined that “the mechanism has been ineffective. Both quantitatively and qualitatively, the implementation of Safe Harbor has been embarrassingly weak. US companies find the Safe Harbour process cumbersome while the resulting data protection is confused and often wholly insufficient. Since companies see a lack of resolve on the part of the European Union to enforce the European data protection regime, the use of Safe Harbor for compliance has few tangible incentives.”

The various criticisms by different stakeholders since the inauguration of the Safe Harbour regime would seem to merit further assessment by the Commission as to adequacy of the regime and, if these criticisms are deemed to be valid, then the Commission should renegotiate the terms of the Safe Harbour agreement with the US.

**Binding Corporate Rules**

Most global firms have European offices and activities as well as commercial activities in third countries and are usually interested in ongoing transfers of data between offices around the world. The data might be about employees, consumers or potential consumers.

An alternative to the Safe Harbour agreement are the so-called Binding Corporate Rules (BCRs). Article 26(2) of the Directive permits multinational corporations to export personal data under BCRs, which are a code of conduct on the extra-European processing of data adopted and implemented by the multinational. To be approved, the BCRs should comply with the Directive’s principles. The BCRs are expected to describe for what purposes the group (the multinational company) will process personal data and to be sufficiently detailed to enable data protection authorities to assess if the level of protection is adequate.

BCRs suffer from several problems. At present, the process of approval is rather long, cumbersome and expensive, though there are intense efforts to streamline the process. Second, BCRs are limited in their scope to particular corporate transfers of data. They do not offer a universal solution to all data protection issues. Third, the multinational firms are likely to push for a lower level of data protection. Fourth, BCRs might conflict with local laws. Fifth, enforceability and compliance are difficult to achieve. Lastly, implementation within the multinational company is yet another difficulty, especially given the dynamic nature of global business.

The Article 29 Data Protection Working Party found other problems with BCRs. International companies do not understand the BCRs, nor what is expected by them, and/or are concerned

---


by the length of the approval process. Moreover, most data protection authorities face a lack of staff dedicated to BCRs. Nevertheless, European data protection authorities meeting in Paris in June 2008 concluded that there was no alternative to BCRs for global companies in order to legally cover international data transfers within their group.468

The Working Party said that BCRs and the ways to complain and seek a remedy for a breach of the rules should be easily accessible by the individual (the “data subject”).

5.4.4 APEC

The challenge of reconciling two goals – to protect personal data and to ease global transfers of data – present in the OECD guidelines may also be seen in the Privacy Framework promulgated by the Asia-Pacific Economic Cooperation (APEC) in 2005469 -- and for the same reason too – the US influence. The 21 member countries adopted nine privacy principles: preventing harm, integrity of personal information, notice, security safeguards, collection limitations, access and correction, uses of personal information, accountability, and choice. Like the OECD and Council of Europe, APEC aims to balance the goals of protecting privacy and enabling information flows. According to the Framework, a data controller should obtain the data subject’s consent for transferring the data to a third party.470

APEC says its Privacy Framework aims to promote a consistent approach to information privacy protection, avoid the creation of unnecessary barriers to information flows and prevent impediments to trade across APEC member economies. The Framework provides technical assistance APEC members that have not yet adopted a privacy policy or regulations. Under the Framework, APEC is helping its members with privacy action plans, identifying best practices and the role of trust-marks in promoting the cross-border flow of information. In September 2007, APEC Ministers approved the APEC Data Privacy Pathfinder, a commitment in support of collaborative projects aimed at accountable cross-border information flows under the guidance of APEC principles. The Data Privacy Pathfinder is expected to promote consumer trust and business confidence in cross-border data flows, reduce compliance costs, provide consumers with effective remedies and minimise regulatory burdens.471

APEC says new and flexible approaches to accountability and compliance are needed if members are to implement its Privacy Framework. Cross-border privacy rules (CBPRs) are expected to facilitate flexible cross-border information flows within a system that ensures credible oversight and enforcement of the CBPRs. The Pathfinder projects are expected to build a system that allows businesses to create their own CBPRs and consumers to rely upon ‘accountability agents’, as well as regulators, in the APEC region to make sure businesses are held accountable to their privacy promises. Accountability agents are any organisation that certifies the compliance of business-developed CBPRs within the APEC framework and/or

471 http://www.apec.org/apec/apec_groups/committee_on_trade/electronic_commerce.html
provides a dispute resolution service if consumers have privacy complaints with business. An accountability agent may be a regulator, such as a privacy commissioner. The term also includes privacy trustmarks, which are in use in some APEC countries, as well as other organisations, for example, government agencies or ministries that may be distinct from a regulator but which fulfil this role. While Ministers have endorsed the Pathfinder, this does not mean that all countries are required to participate in all or any of the Pathfinder projects. APEC recognises that its members are at differing levels of development and implementation of privacy frameworks within their economies.472

Canadian Privacy Commissioner Jennifer Stoddart observed recently that the Pathfinder projects are attempting to develop a set of accountability mechanisms that would apply to transborder flows and facilitate co-operation among enforcement authorities. At a minimum, she said, the APEC process is exposing APEC members that don’t yet have privacy regimes to principles and concepts which will be helpful as they develop domestic laws. This may encourage a “bottom-up” approach to privacy protection that reflects APEC’s diversity.473

5.4.5 International Conference of Data Protection and Privacy Commissioners

The International Conference of Data Protection and Privacy Commissioners has become an important forum for discussions and resolutions on international transfers of personal data. It has called for greater transparency with regard to the collection of passenger data. Meeting in Montreal in September 2007, the conference adopted a Resolution calling upon governments to be open and transparent about the purposes for which data are collected and used and to make sure all passengers, regardless of their citizenship or country of origin, are provided with access to their personal information and appropriate redress mechanisms. It also said any government programmes using passenger data should provide for data minimisation; explicit limits on use, disclosure and retention appropriate to the purpose of the programme; data accuracy, rights of access and correction and independent review. It said if governments do not take an approach which correctly weighs data protection and privacy concerns, there is a real danger they will undermine the very fundamental freedoms they are seeking to protect.474

In October 2008, the International Conference agreed to establish a working group to draft a proposal for setting international standards on privacy and personal data protection, which will be submitted to the 31st conference. Among other things, the proposal would formulate “the essential guarantees for better and flexible international transfers of data”.475

5.5 FURTHER RESPONSES NEEDED

Reidenberg, among others, reckons that an appropriate response to the challenges posed by international transfers of personal data would be an international treaty, which he suggests be established within a WTO framework. While the idea of an international treaty has merit, negotiating it within the context of the WTO would make privacy a trade issue whereas it is better seen as a human rights issue (which is how Europe has seen it, c.f., Article 8 of the Charter of Fundamental Rights of the European Union).

The EDPS has said further work is needed with regard to ensuring an adequate level of protection for exchanges with third countries according to a common EU standard and has urged EU institutions to begin work on further improvements on the framework for data protection in law enforcement as soon as possible.476

The International Conference of Data Protection and Information Commissioners are interested in international privacy and data protection standards, and work along these lines is taking place within the ISO.

There may eventually be a new international agreement covering international transfers of personal data, which could effectively replace the patchwork of solutions on offer so far – the contractual arrangements, Safe Harbour agreement, BCRs and initiatives such as the High Level Contact Group.

But further responses seem warranted.

One problem with many “solutions” to date has been the lack of consultation with stakeholders. Such consultation should take place in the context of a privacy impact assessment.

A second problem is the lack of an audit, especially a regular audit, of the measures that are supposedly designed to protect personal data after they have been transferred beyond EU borders. Even occasional random audits of companies that have self-certified under the Safe Harbour agreement would help restore some credibility to the agreement and its intent.

Some metrics would also help to inform stakeholders about how successful the measures are. For example, it would be useful to measure the number of requests for access to personal data held in third countries, the time it takes to get access, the costs involved, the number of corrections made, how often or the number of instances in which personal data are passed on to other organisations, etc.

As the Article 29 Working Party has recommended, travellers should be informed in advance of their confirmation of a booking that the US (for example) will be collecting their details, including some biometrics and may inspect the contents of their laptops, mobiles and Blackberries. Better visibility of similar warnings posted on websites would help to alert users that their data will be transferred to third countries.

There should be provision for accountability and enforcement measures in any agreements involving the transfer of personal data.

6 LEGAL CHALLENGES

This section analyses a series of key challenges faced by privacy and data protection rules in the context of the emergence of the ubiquitous Information Society. Recent, current and expected developments highlight a series of potential limitations of the current EC regulatory framework for the protection of private life and personal data. Such limitations have sometimes been illustrated by national legal or jurisdictional initiatives.

One of the main legal texts in the current regulatory framework is Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector.477 Directive 2002/58/EC, generally referred to as the e-Privacy Directive, replaced Directive 97/66/EC,478 and had to be transposed into national law by Member States by 31 October 2003 at the latest.


The EC adopted on 13 November 2007 a proposal to amend Directive 2002/58/EC.482 The proposal introduces a series of amendments relating to breach notification, better protection against spam and malware, and better enforcement. Such amendments are not discussed in the present study, which focuses on pending issues and other challenges.

6.1 CHALLENGES RELATED TO KEY DATA PROTECTION NOTIONS

A first group of challenges relates to the eventual need to review certain data protection notions in the light of current and expected developments.

---

6.1.1 Definition of personal data

The definition of “personal data” is at the core of the protection granted by the Data Protection Directive, and complimentarily, by the e-Privacy Directive. It has a direct impact on the scope of application of Directive 95/46/EC, which is described in its Article 3(1) as applying to “the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system”.

The Data Protection Directive defines in Article 2(a) “personal data” as “any information relating to an identified or identifiable natural person (‘data subject’); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity”. The e-Privacy Directive does not foresee any specific definition of ‘personal data’, and therefore the definition of Article 2(a) of Directive 95/46/EC applies also for its purposes. Other international legal instruments provide definitions of the notion personal data. Article 2(a) of Convention 108 of the Council of Europe defines “personal data” as “personal data” means “any information relating to an identified or identifiable individual ("data subject")”.

The interpretation of the EC definition of personal data has not been consistent in all Member States, or among different actors. Aware of the existence of divergences in Member States, the EC called in 2003 for the Article 29 Working Party to sustain its contributions to achieving a more uniform application of the Directive. In its 2007, the EC acknowledged that certain divergences persisted, and repeated its call on the Article 29 Working Party for ensuring better and more coherent implementation, calling also on national data protection authorities to adapt their domestic practice to the common line decided in the context of the Working Party.

The Article 29 Working Party adopted on 20 June 2007 an Opinion on the concept of personal data aimed at coming to a common understanding of the concept of personal data, the situations in which national data protection legislation should be applied, and the way it should be applied. In the document, the Working Party takes as a starting point that the definition to be found in the Data Protection Directive reflects the intention of the European lawmaker to provide a wide notion of “personal data”. It then analyses in detail the main different elements or “building blocks” of the definition, namely “any information”, “relating to”, “an identified or identifiable” and “natural person”.

---

483 See Art. 2 of Directive 2002/58/EC.
486 Ibidem, p. 23.
489 Ibidem, p. 3.
490 Ibidem, p. 4.
491 Ibidem, p. 6.
The terms “identified” and “identifiable” have been notoriously subject to divergent interpretations. Industry has generally tended to consider as data related to identified or identifiable persons only the data providing a stable point of contact with the individual. Processing of data related to individuals whose names are unknown or who cannot be contacted therefore tends to be regarded as not representing an interference with their private life, from this perspective.

European case law currently provides limited references for the interpretation of “personal data.” National case law reflects divergent perspectives, from instance in the British Durant case and the Belgian Court of Cassation judgement of 27 February 2001.

6.1.2 Definitions of data controller and data processor

Directive 95/46/EC establishes “data controllers” and “data processors” as responsible entities for compliance with the Directive’s provisions. “Data controllers” are defined in Article 2(d) of the Data Protection Directive, and “data processors” in Article 2(e). Applications such as social networking sites tend to blur the distinctions between service providers (“authors” or “editors”) and users/consumers (or “readers”). It remains to be determined whether the concept of controller as it exists in the current European legal framework for data protection is still relevant and operational when end users are progressively becoming more important actors in the processing of personal data. Moreover, new technological developments tend to put under pressure the distinction between data controllers and data processors as established by Articles 2(d) and 2(e) of the Data Protection Directive.

---

492 For an overview, see Poullet, Y., and J.-M. Dinant, Rapport sur l’application des principes de protection des données aux réseaux mondiaux de télécommunications: L’autodétermination informationnelle à l’ère de l’Internet, Comité Consultatif de la Convention pour la Protection des Personnes à l’Égard du Traitement Automatisé des Données à Caractère Personnel, Conseil de l’Europe, Strasbourg, 18 November 2004, p. 30. The notion of “relating to” is also subject to different interpretations; the Article 29 Working Party’s view is that data can relate to an individual when they are about an individual (content element), when processed for an individual (purpose element) and when processed with an effect on an individual (result element).


6.2 CHALLENGES FOR BETTER IMPLEMENTATION

A second group of challenges relates to the eventual convenience of up-dating certain aspects of current legislation, in particular as a response to the pressures imposed on implementation of existing legislation.

6.2.1 Scope of application of Directive 2002/58/EC

Directive 2002/58/EC applies to “the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community” (Article 3). The definitions of “electronic communications network”, “electronic communications service” and “public communications network” are provided by Article 2 of Directive 2002/21/EC. Even if some of the provisions of Directive 2002/58/EC are generally applicable, most of them concern the responsibilities of providers of publicly available electronic communication services, and this limitation can be envisioned as problematic, as it does not take into account the increasing importance of private communication networks, nor the need to protect individuals from being monitored in such circumstances. Nor does it take into account the progressive blurring of public and private communications networks.

The Directive’s limitations have been underlined especially in reference to RFID. Despite the recent proposal to include an explicit reference to RFID in an amended e-Privacy Directive, RFID would still remain partially uncovered (i.e., RFID not connected to publicly available electronic communications services in public communications networks).

Additionally, it needs to be taken into account that certain actors playing increasingly relevant roles in electronic communications are not providers of electronic communications services, but Information Society service providers, or play mixed roles. The Article 29 Working Party has acknowledged, for instance, that in the context of the Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the

---

498 Article 5 on the confidentiality of communications and Article 13 on spam.
502 As defined by Article 2(a) of Directive 2000/31/EC.
internal market (Directive on electronic commerce), search engine providers must be considered as a type of information society service provider, namely providers of “information location tools”. However, the Working Party considers that, inasmuch they process personal data, search engine providers must be considered data controllers, and when a search engine provider offers an electronic communication service such as a publicly accessible e-mail service, the service is subject to the e-Privacy Directive.

The legal qualification of the different actors playing a role in the ubiquitous Information Society might need to be rethought in the light of current developments, and particular consideration should be given to who should be responsible for compliance with privacy and data protection rules. The limitations of the scope of application of Directive 2002/58/EC also affect the protection granted to two specific categories of data, namely ‘traffic’ and ‘location’ data.

6.2.2 On traffic and location data

Article 2(b) of Directive 2002/58/EC defines traffic data as “any data processed for the purpose of conveyance of a communication on an electronic communications network or for the billing thereof”. The definition, it shall be noted, does not include any reference to the concept of personal data. Article 6 establishes that traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when they are no longer needed for the purpose of the transmission of a communication. This also applies to all location data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof [Article 2(b)]. Recital 35 clarifies that this concerns location data giving the geographic position of the terminal equipment of the mobile user processed to enable the transmission of communications, which therefore are to be considered traffic data covered by Article 6. Traffic data not falling under the scope of Directive 2002/58/EC might fall under the scope of Directive 95/46/EC when considered personal data. Traffic data not falling under any of the legal instruments remain unprotected.

Data that can be considered traffic data include notably Internet protocol (IP) addresses. In practice, IP addresses are being increasingly processed by entities that do not consider them to be personal data, and therefore do not consider themselves ‘data controllers’ in the sense of the Data Protection Directive. The Article 29 Working Party has reacted to these practices by asserting that in most cases, including cases of dynamic IP address allocation, the user(s) of the IP address are identifiable. In its view, Internet service providers, as well as search engine operators, should treat all IP data as personal data unless completely sure of being able to determine that the data corresponds to users that cannot be identified. The massive collection of traffic data by social network providers represents in any case a key challenge to privacy in this context, especially as in some cases the traffic data resemble location data.

Challenges raised by the processing of IP addresses could be intensified in the context of the

---

introduction of new protocols such as IPv6, allegedly leading to increased risks of profiling of user activities on the Internet, as well as increased risks linked to security and confidentiality issues.\footnote{The risks are actually dependent on the configuration of the protocol. See International Working Group (IWG) on Data Protection in Telecommunications, \textit{Working Paper on the use of unique identifiers in telecommunication terminal equipments: the example of IPv6}, Auckland, 26-27 March 2002.}

Equivalent considerations can be developed in reference to location data. Article 2(c) of Directive 2002/58/EC defines location data as “\textit{any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service}”. The definition does not include any reference to the concept of personal data. Recital 14 of Directive 2002/58 also refers to location data by the sole reference to the terminal equipment of a user. Location data are regulated by Article 9 of Directive 2002/58/EC, which establishes specific conditions for the provision of certain location-based services, i.e., those using location data not covered by Article 6 of the e-Privacy Directive (and not considered traffic data). The processing of location data is permitted when the data are made anonymous, or with the consent of the user or subscriber. Prior to that consent, the user or subscriber has to be informed of the types of data processed, the purpose and duration of the processing, and whether the data will be passed on to third parties. In addition, the user or subscriber must have the possibility of temporarily refusing the processing of location data. The only exceptions to the principle of prior consent are the use of location data by emergency agencies (Article 10(b) of the e-Privacy Directive) or by law enforcement authorities (Article 15.1 of the e-Privacy Directive). Location data not falling under the scope of Directive 2002/58/EC might fall under the scope of Directive 95/46/EC when considered personal data. Location data not falling under either Directive remain unprotected. The use of location data has remarkably increased in the last years, notably driven by the use of satellite location data and mobile technology.\footnote{Article 29 Data Protection Working Party, Opinion on the use of location data with a view to providing value-added services, WP 115, November 2005. \url{http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp115_en.pdf}}

Through the emerging technology of content-based image retrieval (CBIR), location-related data can be obtained from data not initially regarded as location data.\footnote{IWG, op. cit., p. 3.}

\section*{Modalities of consent}

Consent\footnote{For a general discussion of the weaknesses of consent from a theoretical perspective, see: Serge Gutwirth, \textit{Privacy and the information age}, Rowman & Littlefield Publ., Lanham/Boulder/New York/Oxford, 2002.} plays a very important role in relation to various provision of the EC legal framework for privacy and data protection. It shall be emphasised, however, that consent is not a tool allowing for the suspension of other data protection obligations, and that it can never represent by itself a sufficient ground for legitimate processing, which is always subject to other requirements such as, most notably, proportionality.

The Data Protection Directive defines “the data subject consent” in Article 2(h), as “\textit{any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relation to him being processed}”. Article 7 (a) of the Data Protection Directive foresees “consent” as one of the criteria for making processing legitimate,\footnote{Processing can also take place based on other grounds, such as \textit{ex contractu} (Art. 7(b) of Directive 95/46/EC), \textit{ex lege} (Art. 7(c)) or for the protection of the vital interests of the data subject (Art. 7(d)), among others.} allowing processing to take place if the data subject has unambiguously given
his consent to it. The Article 29 Working Party stressed in its Working document on data protection and privacy implications in eCall initiative\textsuperscript{511} that such consent “shall be ‘freely given’ and should also allow the data subject the opportunity to withdraw consent”, as well that “the consent would not be freely given if the data subject has to accept a clause in this regard in the framework of a contract of non-negotiable clauses”. National legislation can in certain cases not allow for consent to be a valid ground for the collection or processing of personal data.

The Data Protection Directive also refers to consent in Article 8(2), allowing for the general prohibition of the processing of special categories of data\textsuperscript{512} to be lifted when the data subject has given “explicit” consent to such processing, unless Member States have provided otherwise. Additionally, Article 26(1) of the Data Protection Directive stipulates that, save where otherwise provided by domestic law, transfers of personal data to third countries not ensuring adequate levels of protection for personal data can take place when “(a) the data subject has given his consent unambiguously to the proposed transfer”.

In the e-Privacy Directive, consent is also referred to in different provisions, and notably in Article 9, on the processing of location data other than traffic data. Article 9(1) introduces consent of the users and subscribers as one of the grounds allowing for the processing of such data, and Article 9(2) adds that where consent has been obtained for the processing of such data, the “user and subscriber must continue to have the possibility, using a simple means and free of charge, of temporarily refusing the processing of such data (…)”. Article 13(1) of Directive 2002/58/EC conditions the use of automated calling machines, fax and electronic mail for direct marketing purposes for the cases where the subscriber has given prior consent. Moreover, Article 5(3) establishes that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned are offered the right to refuse such processing.

Additionally, different international instruments foresee special provisions regarding consent. Recommendation No. R (97)5 of the Council of Europe on the Protection of Medical Data,\textsuperscript{513} for instance, establishes in Art. 6(1) that where the data subject is required to give his/her consent, “this consent should be free, express and informed”.

It has been suggested that providing personal data as a condition of access to a site or an online service could be viewed not merely from the standpoint of data protection legislation but also from that of consumer law, in terms of unfair practices in obtaining consent or the major detriment arising from the imbalance between the value of the data secured and that of the services supplied.\textsuperscript{514} Consent of minors requires special attention, especially, for example, in the context of their heavy participation in social networking, the activities of which

\textsuperscript{511} Article 29 Data Protection Working Party, Working document on data protection and privacy implications in eCall initiative, WP 125, Adopted on 26 September 2006.  
\textsuperscript{512} In particular, data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life (Art. 8(1) of the Data Protection Directive).
\textsuperscript{513} Adopted by the Committee of Ministers on 13 February 2007.
increasingly rely on location data (for instance, in mobile virtual communities). Moreover, the cases in which adult subscribers monitor minors represent a special challenge.\footnote{Indeed, parental consent can sometimes dangerously transform itself into a mechanism enabling parents to exercise control over children. See: International Working Group (IWG) on Data Protection in Telecommunications, \textit{Working Paper on Children’s Privacy On Line: The Role of Parental Consent}, Auckland, 26-27 March 2002.}

The main challenge regarding these provisions on consent is how to apply them in the context of the ubiquitous information society in practical terms. How should “explicit” consent be expressed, and proved? What about “unambiguous” consent? Is consent of users to treated differently or similarly to consent of subscribers? What conditions should comply with the effective possibility of withdrawal of consent? What are the requirements of effectively offering a right to refuse to the use of cookies?\footnote{Article 10 of Directive 95/46/EC establishes that “Member States shall provide that the controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it: (a) the identity of the controller and of his representative, if any; (b) the purposes of the processing for which the data are intended; (c) any further information such as the recipients or categories of recipients of the data, whether replies to the questions are obligatory or voluntary, as} The practical modalities of consent are not regulated in any detail at EC level, leaving many questions open and subject to divergent interpretations.

\subsection*{6.2.4 Applicable law}

The e-Privacy Directive lacks any provision equivalent to Article 4 of the Data Protection Directive regarding applicable national law. Thus, said Article 4 is the one to be used to determine the applicable law both under the Data Protection Directive and the e-Privacy Directive. Article 4, however, appears to be extremely ill-suited in the light of certain current and expected developments. The difficulties appear in particular in reference to Article 4(1)(c), which provides that when the data controller is not established on Community territory but, for the purposes of the processing personal data, makes use of equipment situated on the territory of one Member State, said Member State shall apply its national provisions to the processing in question, unless the equipment is used only for purposes of transit.

The Article 29 Working Party has noted that search engines generally use cookies and that, in its view, cookies should be regarded as “use of terminal equipment”. Thus, in its analysis, the Data Protection Directive applies to the processing of personal data by search engine providers even when their headquarters are outside the European Economic Area (EEA).\footnote{European Data Protection Supervisor, \textit{Annual Report 2007}, Brussels, 15 May 2008, p. 57.}

The fragility of this argumentation (which can be invalidated through the collection of data by means other than cookies) contrasts with the increasing relevance of processing by search engines of personal data. Complexity increases as remote data storage and web applications render even more problematic the concept of the “location” of the process.\footnote{Article 29 Data Protection Working Party, Opinion on data protection issues related to search engines, 00737/EN, WP 148, Adopted on 4 April 2008, p. 11. \texttt{http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp148_en.pdf}}

\subsection*{6.2.5 Transparency requirements}

Article 10 of Directive 95/46/EC lists the information obligations for the data controller in case of collection of data from the data subject,\footnote{Article 29 WP, Opinion 8/2006, op. cit.} and Article 11 enumerates the requirements
where the data have not been obtained from the data subject. These requirements are increasingly difficult to apply and increasingly neglected or ignored. Social networking sites have been identified as especially problematic, as users tend not to be aware of all the data collected about them. The transparency of profiling and data mining practices represents also a key legal challenge, as does the articulation in practice of information requirements and the conditions for the validity of consent.

6.3 OTHER LEGAL CHALLENGES

6.3.1 Dealing with the processing of “unprotected” data

A vast amount of data processed in the ubiquitous information society might not be clearly personal data, but rather “electronic footprints” whose qualification as “personal data” is not self-evident. Those “electronic footprints”, however, can undoubtedly be used to influence groups and individuals. Today, using data mining and profiling techniques, one can obtain profiles of subjects without processing any data strictly related to an identified or identifiable person. Data used to build the profiles can simply relate to devices or even files accessed. However, the processing may be an interference with the individual’s private life, either because of the constant monitoring it requires, the consequences of the profiling or the decisions taken based on the profile obtained. The legal challenge in this context is how to avoid these practices taking place outside the scope of any provisions on privacy or data protection.

The use of identifiers is especially challenging. There are different types of identifiers. IP addresses are an example of communications identifiers, which are to be considered as personal data in a majority of cases but not always, in the view of the Article 29 Working Party. Not all electronic communications rely on IP addresses, and other identifiers might increase in importance as services converge. For various reasons, including security, devices can have unique identifiers, and it has been proclaimed that in a not too distant future every single object might be identifiable and addressable. Already now, an important amount of components of computers include identifying numbers. Files also can be uniquely identified, and can include device identifiers. Moreover, file data can be enriched with metadata. Image files, for instance, are automatically embedded by many cameras with metadata about the camera itself, including in certain cases the serial number of the camera. The serial number of the camera can be linked to an address or other data through warranty registration cards. Location data can also be embedded in digital files by the devices used to produce them. We

well as the possible consequences of failure to reply, the existence of the right of access to and the right to rectify the data concerning him, in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.”

520 IWG’s ‘Rome memorandum’, op. cit.


522 For the concerns of data protection authorities on the global proliferation of profiling practices, see International Working Group (IWG) on Data Protection in Telecommunications, Resolution on Privacy Protection and Search Engines, 28th Conference, 2-3 November 2006, London.


can see how problematic it becomes when applications generate user data without the user’s knowledge.

6.3.2 ISPs and the disclosure of personal data

Provisions aiming at the protection of privacy and personal data may conflict with certain other values that the European legislator aims to promote. One of the situations in which a conflict can become apparent in practice is when a right holder is confronted with infringements of her Intellectual Property Rights (IPRs) over the Internet and addresses an Internet service provider (ISP) in order to obtain identification details. In this context, the question arises whether the European legislator has determined whether the ISP has any obligation of disclosure and, if so, under what conditions the ISP is obliged to communicate the personal data of their users in the context of proceedings initiated to enforce IPRs.

Provisions regarding the means to enforce IPRs are set out in Directive 2004/48/EC on the enforcement of intellectual property rights, generally referred to as the Enforcement Directive.525 Article 8 of the Enforcement Directive contains a provision relating to the IPR-holder’s right to information and requires the Member States to provide the legal tools that allow a judge, in response to a justified and proportionate request, to order that information on the origin and distribution networks of the infringing services or goods be communicated to the claimant. This obligation can be imposed on, inter alia, ISPs [Article 8.1(c) of the Enforcement Directive]. The information can relate to the names and addresses of infringers or the scope of the counterfeit. This right to information can enable the right holder, for example, to identify users of peer-to-peer file-sharing services who infringe the copyrights and related rights vested in musical or audiovisual content and to bring action against these individuals. However crucial it may be for the effective enforcement of IPRs, such a strategy nevertheless raises important privacy concerns. Consequently, the Enforcement Directive states that the obligation of the Member States to provide this right to information should not curtail, inter alia, the (national) legislation relating to the processing of personal data [Article 8.3(e) Enforcement Directive].

The Enforcement Directive leaves it to the Member States to strike a balance between the interests of the IPR-holders and the individuals whose personal data may be shared. Article 15 of the e-Privacy Directive allows for restrictions of privacy for reasons of “national security (i.e., State security, defence, public security and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system”. Article 13(1) of the Data Protection Directive also provides for restrictions in the protection of personal data, different from those in the e-Privacy Directive: it notably allows a limitation in order to safeguard the “protection of the rights and freedoms of others”, which includes intellectual property rights of third parties. Under this umbrella, Member States are allowed to provide an exception to the protection of personal data in favour of the enforcement of IPRs. Article 15(1) of the e-Privacy Directive includes a reference to Article 13(1) of the Data Protection Directive.

The European Court of Justice (ECJ) has examined the obligations on ISPs to disclose details concerning their users and the enforcement of IPRs in the “Promusicae / Telefónica” case.526

In this case, an association of rights holders sought an injunction against an Internet service provider to communicate the names and addresses of users whose IP addresses the association had retrieved and whose identities it wanted to obtain from the ISP. While Spanish law contained the obligation to communicate the identities of infringers in the context of criminal proceedings, it lacked provisions for this possibility in civil proceedings. In a preliminary procedure, a Spanish commercial court asked the ECJ “whether Community law … must be interpreted as requiring Member States to lay down, in order to ensure effective protection of copyright, an obligation to communicate personal data in the context of civil proceedings”. The ECJ ruled that this was not the case.

The Court examined whether national legislation imposes an obligation to communicate personal data in order to allow the claimant to bring civil proceedings and whether a copyright infringes the e-Privacy Directive. Advocate General Kokott read Article 15 of the e-Privacy Directive restrictively\(^\text{527}\): she concluded that the “rights of others” (as stated in Article 13 of the Data Protection Directive) were not included in the list of authorised restrictions. She concluded, however, that it is compatible with Community law for Member States to exclude the communication of personal traffic data for the purpose of bringing civil proceedings against copyright infringements, if it is necessary to ensure “public security” [Article 15(1) of the e-Privacy Directive], provided that traffic data are not directly surrendered to the right holders but pass through the hands of the competent state authorities (such as data protection authorities) and that the communication of personal data is excluded for trivial cases.\(^\text{528}\) Unlike the Advocate General, the ECJ considered that, since Article 15(1) of the e-Privacy Directive refers to Article 13(1) of the Data Protection Directive, the Member States are allowed to restrict the protection of personal data on the grounds listed in this latter provision, inter alia, for the protection of rights and freedoms of others. Having decided that national legislation providing an obligation to communicate personal data in civil proceedings is compatible with Community law, the ECJ then considered whether Community law requires the Member States to provide such an obligation. Examining Directives 2000/31/EC, 2001/29/EC\(^\text{529}\), 2004/48/EC and 2002/58/EC, the ECJ concluded that Community law does not require Member States to lay down an obligation to communicate personal data in order to ensure effective protection of copyright in the context of civil proceedings. However, if they do, Member States are required to strike a fair balance between the various fundamental rights protected by the Community legal order.

A related question has been raised again in another case, currently pending before the ECJ.\(^\text{530}\) These developments take place in the context of a wider debate on the role of ISPs regarding content delivery. In certain Member States, there is a trend towards a greater role for ISPs in enforcing copyrights.\(^\text{531}\) Such a role could consist of filtering and blocking illegal content, sanctioning users for copyright infringements (i.e., by refusing access to the Internet) or

---

\(^{527}\) Opinion of Advocate General Kokott, delivered on 18 July 2007 in case C-275/06, Promusicae, point 89.

\(^{528}\) Points 107-112 of the Opinion.


\(^{530}\) Reference for a preliminary ruling from the Oberster Gerichtshof (Austria) lodged on 14 December 2007 - LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH v Tele2 Telecommunication GmbH, Case C-557/07, OJ C 64, 08.03.2008, p.20.

\(^{531}\) For example, see CBS et al., “Principles for User Generated Content Services”, 18 October 2007, http://www.ugcprinciples.com. In Europe, ISPs have already been obliged to take measures against the transmission of illegal files, e.g., the P2P site RapidShare (based in Switzerland) was condemned by a German Court, and the Belgian Internet service provider Scarlet was condemned in Belgium.
bringing into effect sanctions imposed by another authority. This trend, facilitated by techniques such as deep packet inspection, can have implications for the right to privacy and, more particularly, for the right to confidentiality of communications.

### 6.3.3 Confidentiality of communications and integrity of information systems

The only provision in the EC regulatory framework recognising a right to the confidentiality of communications is Article 5 of Directive 2002/58/EC, which establishes that:

1. Member States shall ensure the confidentiality of communications and the related traffic data by means of public telecommunications network and publicly available telecommunications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications, by others than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.

The Article 29 Working Party has underlined that this Article imposes an obligation to ensure confidentiality of communications irrespective of the nature of the network and whether the communication crosses borders to non-EU member states. The recognition of this right, however, appears not to be clear enough regarding the duties and transparency obligations of the different providers potentially involved, especially in the context of the ubiquitous Information Society. This might lead to a lack of effective protection of the right to privacy of communications, granted by Article 7 of the European Charter of Fundamental Rights, as well as by the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR). A development possibly requiring special attention in this area is VoIP.

The right to confidentiality enjoys constitutional protection in certain Member States, which generally base the protection on a prohibition of interference, regardless of the personal or private character of the communication. This is particularly relevant as the compliance with

---

532 See the French report on “Le développement et la protection des œuvres culturelles sur les nouveaux réseaux” (the “Olivennes” report) of November 2007. See also section 3.1.5 above and, in particular, the citation Dumons, Olivier, “Téléchargement : les géants de l'Internet en croisade contre le projet de loi Olivennes”, Le Monde, 7 May 2008. [http://www.lemonde.fr/technologies/article/2008/05/07/telechargement-les-geants-de-l-internet-en-croisade-contre-le-projet-olivennes_1041771_651865.html#ens_id=1041790](http://www.lemonde.fr/technologies/article/2008/05/07/telechargement-les-geants-de-l-internet-en-croisade-contre-le-projet-olivennes_1041771_651865.html#ens_id=1041790). The European Parliament, in point 23 of its recent Resolution of 10 April 2008 on cultural industries in Europe [2007/2153(INI)], “calls on the Commission and the Member States to recognise that the Internet is a vast platform for cultural expression, access to knowledge, and democratic participation in European creativity, bringing generations together through the information society; [and] calls on the Commission and the Member States to avoid adopting measures conflicting with civil liberties and human rights with the principles of proportionality, effectiveness and dissuasiveness, such as the interruption of Internet access’’.


534 Article 7 of the European Charter of Fundamental Rights states: “Everyone has the right to respect for his or her private and family life, home and communications.”


536 For instance, in the Netherlands through Article 13 of the Dutch constitution.
data protection provisions by information service providers (based on the protection on personal data) is clearly not equivalent to the protection granted by the right to confidentiality of communications. The question remains of how to ensure that the confidentiality of communications is respected in cases in which the communication takes place under the responsibility of an information service provider (for instance, when messages are exchanged via social networking sites). Paradoxically, a special challenge to the right to the confidentiality of communications might be the development of technologies for the reinforcement of the security of communications.\footnote{International Working Group (IWG) on Data Protection in Telecommunications, *Working Paper on Intrusion Detection Systems (IDS)*, Berlin, 2-3 Sept 2003.}

Article 5(3) of Directive 2002/58/EC establishes that

> Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.

Even though it is placed under the heading “Confidentiality of communications”, this provision actually refers to the protection of information stored in the terminal equipment.\footnote{The protection of communications encompasses the protection of communications while being transported and the protection of stored communications. See Koops, Bert-Jaap, “The shifting ‘balance’ between criminal investigation and privacy: A case study of communications interception law in the Netherlands”, *Information, Communication & Society*, Vol. 6, Issue 3, Sept 2003, pp. 380-403. http://www.informaworld.com/smpp/title~content=g713768656~db=all}

The exact scope of the protection can be interpreted in different ways. On one hand, the provision refers to information stored (note that it is not limited to the protection of personal data)\footnote{In this sense, see Debusseré, F., “The EU E-Privacy Directive: A Monstrous Attempt to Starve the Cookie Monster?”, *International Journal of Law and Information Technology*, Vol. 13, No. 1, 2005, p. 83. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=915206 or http://ijlit.oxfordjournals.org/content/vol13/issue1/index.dtl} but, on the other hand, it refers to processing by the data controller, a category which can only be defined in reference to personal data. The Article 29 Working Party is of the view that Article 5(3) (as well as Article 13) is a general provision applicable not only to electronic communication services but also to any other services when these techniques are used.\footnote{Article 29 Working Party, Opinion on data protection issues related to search engines, 4 April 2008, WP 148. Budapest, 23.11.2001.}

Different provisions might be implemented at national level also in reference to the obligations imposed by the Convention on Cybercrime of the Council of Europe\footnote{Article 29 WP, Opinion 8/2006, op. cit., p. 3.} in relation to offences against the confidentiality, integrity and availability of computer data and systems.

Article 5(3) of the e-Privacy Directive can be interpreted as related to Recital 25 of the same Directive, in which cookies are mentioned. The approach to the regulation of cookies introduced in Recital 25 has however been criticised as inconsistent, as it acknowledges the right to refuse cookies and, at the same time, the possibility to make access to a website conditional on the acceptance of cookies.\footnote{http://papers.ssrn.com/sol3/papers.cfm?abstract_id=915206 or http://ijlit.oxfordjournals.org/content/vol13/issue1/index.dtl}
On this issue, it is especially worth noting the German Constitutional Court’s judgement on the constitutionality of secret online searches of computers by government agencies.\textsuperscript{543} The judgement derives from a constitutional complaint against a statute allowing the search of IT systems, and questioning the legitimacy of monitoring personal computers without the knowledge of the parties involved. The Court acknowledged a gap in the legal protection of the confidentiality and integrity of personal IT systems\textsuperscript{544} and, in its judgement, recognised a “basic right to the confidentiality and integrity of information systems” as part of the general personality rights constitutionally protected in Germany. The reasoning of the Court notably took into account the increasing importance of information technology for the development of personality. The Court limited exceptions to the new right to specific cases where “factual indications for a concrete danger” exist for the life, body and freedom of persons or for the foundations of the state or the existence of human beings, and declared that measures could only be implemented after approval by a judge. Moreover, the Court declared that secret online searches must in any case be constrained by ad hoc technical measures that do not interfere with “the core area of the conduct of private life”. This landmark ruling has been considered potentially as influential as the 1983 recognition by the same Court of the “right to informational self-determination”.

\textsuperscript{543} Published on 27 Feb 2008 (\textit{Online-Durchsuchung}, 1 BvR 370/07; 1 BvR 595/07).

\textsuperscript{544} Thus, considered to be not satisfactorily protected by the existing German provisions ensuring the right to informational self-determination and the protection against the interception of post and telephone calls and recording conversations.
7 PRINCIPAL CROSS-CUTTING CHALLENGES

In this chapter, we summarise some of the key challenges mentioned in Chapters 2 to 6. Those chapters dealt with specific technological, socio-economic, administrative and legal developments that pose challenges to privacy and trust. Some of the challenges, for example, repurposing or the secondary use of personal data, appear in two or more specific developments. Hence, in this chapter, the challenges – such as secondary use – can be viewed at a higher, more generic level. In other words, the key challenges summarised in this chapter are issues that appear in several different types of development.

Similarly, some of the technological, socio-economic, administrative and legal developments have spawned several challenges. For example, the push by the Commission and Member States towards development of e-health and, in particular, electronic health records raises several different issues or concerns – about the security of medical data, informed consent, balancing competing social values and so on. Similarly, the use of cookies raises several issues such as informed consent, the enforcement of EU legislation, the international transfer of personal data and user awareness. Thus, some developments are cited as an example of a challenge under one subheading in this chapter and then appear again under another subheading.

Furthermore, it should not be surprising to see that many privacy issues are intertwined, for example, transparency and trust – transparency builds trust, while opacity can undermine it.

7.1 DEFINITIONS – PERSONAL DATA, CONTROLLER AND PROCESSOR

Some have questioned certain interpretations of the definition of personal data in the Data Protection Directive as too “black and white”, i.e., that some data may not seem to be personal until they are linked to other data which also may not seem personal, but the linkage makes it possible to identify a person. The UK Data Sharing Review Report offers some examples.

Everybody seems clear that records kept by reference to traditional identifiers, such as a person’s name and address, are caught by the DPA [the UK Data Protection Act 1998]. However, the situation is far less clear in respect of information such as internet IP addresses or CCTV footage. Information like this could be combined with other information to allow an internet user or person in a piece of CCTV footage to be explicitly identified, but might not in itself constitute ‘personal data’. Organisations seem unclear as to how to treat ‘potential personal data’ like this.

As it stands, data protection is an all or nothing piece of law: either information is personal data and the whole of the legislation applies to it, or it isn’t and none of it does. An obvious solution to this problem, but one which neither the DPA or the European Data Protection Directive seem to allow, is to apply some of the rules of data protection to ‘potential personal data’, but not all of them. In the medium and long term, we would encourage the development of data protection law that can be applied much more flexibly and in particular would press for germane revisions to the Directive, to allow subsequent change to domestic law. However, for practical purposes, the concept of ‘protected personal data’ set out by Sir Gus O’Donnell in his Data Handling Review is attractive. This is defined as any material that links an identifiable individual with information, which if released would put them at significant risk of harm or distress; or that relates to 1000 or more individuals not in the public domain. Sir

From this optic, a clear-cut definition of personal data is problematic. The point to note here is that, in some instances, it depends on how data are processed that determines whether linked data are personal. Thus, it can be difficult to apply the same rules in the same way in all situations.

The debate over whether IP addresses should be regarded as personal data highlights these grey areas. Generally, industry opposes regarding IP addresses as personal data whereas regulators generally do regard IP addresses as personal, just like telephone numbers. It is, of course, possible that several different members of a family will use the same computer at different times, just as they would their home telephone number. But it’s difficult to be categorical about IP addresses, especially since some IP addresses belong to computers in the public domain, in cyber cafes, hotels, libraries, schools and universities and so on, where hundreds of different people may use the same computer in the course of a day. In its 24 September 2008 resolution, the European Parliament has said the Commission should study the issue further and present such proposals as may be appropriate.\footnote{European Parliament legislative resolution of 24 September 2008 on the proposal for a directive of the European Parliament and of the Council amending Directive 2002/22/EC on universal service and users’ rights relating to electronic communications networks, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on consumer protection cooperation (COM(2007)0698 – C6-0420/2007 – 2007/0248(COD)). http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2008-0452+0+DOC+XML+V0/EN&language=EN}

Some have suggested the issue of personal data should be framed in a different way – i.e., rather than focussing on the definition of personal data, perhaps we should focus instead on the consequences that arise when bits of data are associated with a particular person and what might happen when that association is made.

Today it can appear to be as a trivial task for companies such as Google, Facebook and many others to describe someone, their interests, habits, purchases, activities and much else; the companies themselves, however, generally claim that according to their own definitions they do not identify the individuals behind much of the data.

7.2 TRANSPARENT DATA COLLECTION AND USE

7.2.1 Who has my data and what are they doing with them?

A recent UK study estimated that, on average, the citizen appears in some 700 databases\textsuperscript{548}, a fact which immediately begs two questions: Who has our data and what are they doing with them? This point raises other issues: Even if we had a list of all these 700 databases and a contact for each one, how likely or possible is it for the citizen to review the data about him- or herself in so many databases? Should the controllers of these databases or, at least, the government ones, maintain logs of who accesses our data? For example, should the department of motor vehicle licensing or those in charge of electoral rolls maintain such logs? And, if so, for how long should such logs be maintained?

As one might expect, a UK survey suggests that the vast majority of people do want to know who has their data. More than two-thirds of 1,025 adults surveyed in the UK in 2008 claimed that it is very important to them to be told the names of which organisations or government departments hold what kind of information about them, and another 19 per cent said this is quite important.\textsuperscript{549}

The snag is that the Data Protection Directive does not require data controllers or those who originally collect the personal data to inform the individual (the data subject) of those third parties to whom they pass the data. Article 10 of the Directive gives data controllers the choice of whether to identify the recipients or only the “categories of the recipients’ data”. Most data controllers surely prefer the latter course.\textsuperscript{550}

Another related issue which has been raised many times is this: Do people own their own personal data? Who “owns” the personal data supplied by a custo In the interests of better transparency, we agree with and reiterate the UK Data Sharing Review Report’s recommendation that organisations should In the interests of better transparency, we agree with and reiterate the UK Data Sharing Review Report’s recommendation that organisations should mer who wants to get a mortgage, life insurance, a discount on his grocery bill, an extended warranty on a product or a new Internet service? Once people have provided their data to a service provider (for example), do they still own the data? Or does the data now belong to the service provider to do with them what he will? Or is the “ownership” shared? That is, the controller can use the data only for specified purposes and must provide access to the data to the individual so that the data can be corrected if necessary? How can we be assured that the service provider will adequately protect our data?

Who should have rightful access to location data – the person being located or the owner of the devices that enable the localisation or anybody in the vicinity?


\textsuperscript{550} Article 10 says “that the controller or his representative must provide a data subject from whom data relating to himself are collected with … information [about] the recipients or categories of recipients of the data” [italics added]. Even the categories (e.g., “partners” or “affiliated companies”) could be so broad as to be meaningless.
Should RFID “users” be made aware of what the RFID controllers can do and are allowed to do with RFID data?

Who owns information that has been passed through filters and aggregators multiple times?

In the instance of e-health, it is even more difficult to guess who might have access to our electronic health records and how our data might be used. The Telegraph, a UK newspaper, bristled in an editorial in September 2008 when the UK government floated the idea that researchers and pharmaceutical companies could have access to medical records without asking for the consent of the persons whose medical conditions the data records: “That proposal, were it ever to become law, would be an outrageous infringement of every individual’s basic right to protect their privacy and the integrity of their person. Your records belong to you, and the Government is not entitled to use them without your permission.”

But is The Telegraph correct? Do our medical records “belong” to us or to the National Health Service? If they belonged to us, that would imply we could have them expunged, but that won’t happen, especially if we have conditions that might pose a threat to public health.

Insurance companies are big data collectors, not just for health insurance, but also other forms of insurance such as that for cars. With so many sensors and tracking devices in vehicles today, they can monitor not just how many kilometres we drive, but also how fast, whether we use our seat belts, the fuel we consume and so on. Insurance companies can use such data to validate their risk calculations and set premiums for individual customers or refuse others not regarded as good risks. Such data are valuable for others too, such as policy-makers dealing with the environment, markets and transportation as well as technologists and law enforcement authorities. The accumulation of such data makes our digital profiles even more fine-grained and raises obvious privacy concerns.

The issue of who has our data and what are they doing with it is complicated by the mergers and acquisitions taking place within the Internet sector, especially those involving the largest Internet companies – Google, Microsoft, Yahoo and AOL – as well as other media companies such as Rupert Murdoch’s News Corp and Reed Elsevier, owner of the LexisNexis Group. These companies have acquired vast stores of personal data and maybe know more about us than our own mothers. So far, the consolidation within the sector has only been addressed by competition authorities, even though many experts believe that the privacy implications are no less important. Indeed, from our point of view, it is baffling why these mergers, acquisitions and alliances have not been investigated by regulatory authorities in terms of the privacy implications in view of their huge stores of personal data and the millions of users who use their services (whether they know it or not). Among the many issues that regulators have so far not addressed is transfer of personal data from one company to another and/or the how personal data previously held by one company are put at the disposition of another company that acquires it or enters into an alliance with it. Does the convergence of companies,
examples of which are referenced above in section 3.5, lead to new uses of personal data for purposes not originally foreseen (and certainly not by those from whom the data have been collected) when the data were collected originally?

Knowing who has our data is made even more difficult by virtue of the fact that many government departments (as well as industry) outsource the processing of personal data. As an example, the US plans to require airlines from August 2009 to collect biometric data (fingerprints) of those exiting the country. The airlines have complained about the cost burden on them, but privacy advocates are more concerned about the privacy implications and data security arising from imposing the task on airlines, even if they have to forward the data to the Department of Homeland Security within 24 hours.

Outsourcing becomes even more problematic when the processing is undertaken by a foreign company, especially one based outside the EU. The outsourcing risk was perfectly illustrated when UK transport minister Ruth Kelly told Parliament that personal information on 3 million candidates for driver licences was missing after an Iowa subsidiary of Pearson Driving Assessments Ltd., a contractor of the Driving Standards Agency, had “mislaid” a computer hard drive.553

In the interests of better transparency, we agree with and reiterate the UK Data Sharing Review Report’s recommendation that organisations should publish and regularly update a list of those organisations with which they share, exchange, or to which they sell, personal information, including ‘selected third parties’.554

7.2.2 Function creep, secondary use

New business models and services often provide an example of function creep and the secondary use of personal data. Companies such as Google and Amazon providing cloud computing services have at their disposition vast amounts of personal information which they can mine and process for secondary uses, even though they state upfront that their provision of free applications and services on the cloud is conditional upon users allowing the cloud operator some sort of access to this information, for example, for advertising.

Some technologies, designed for one purpose, can be used for a secondary purpose, as exemplified by DRM systems that were intended to secure copyright and intellectual property rights, but can also be used to collect and store personal data so that the industry can see who is doing what and, based on this information, can initiate possible law enforcement actions. The collected consumer data can also be used for consumer profiling.

One of the best examples of secondary use comes from social networking websites, where millions of people post personal data about themselves every day. Such personal data are a treasure trove not only for the social networking website operators but also for those thousands of people and enterprises writing third-party applications for such sites. The data

(c) any further information such as
- the categories of data concerned,
- the recipients or categories of recipients,
- the existence of the right of access to and the right to rectify the data concerning him.”

can be mined and processed in hundreds of ways for profiling users and targeting them with advertising, but also for even more malign purposes such as paedophiles “grooming” adolescents and identity thieves usurping personal data for their illicit profits.

How data portability might lead to new secondary uses has yet to be analysed, but seems to be a good topic for some new research. Users might like the convenience and saving in their time when they want to take their Internet profiles from one social network to another without having to create a new profile, but privacy concerns could easily arise when personal information is shared across different websites. The data portability initiatives of social networking operators are mirrored by virtual world operators, such as Second Life, who are taking initiatives to enable an avatar created in one virtual world to be used in another.

7.2.3 Data concentration

It might seem preposterous to suggest that, in this age when more information is available and being created by more people than ever before, there is a risk that a small (and getting smaller) number of organisations are acquiring more information about more of us. However, arguably, such seems to be the case. First and foremost among those organisations is Google whose stated ambition is to organise the world’s information. In December 2007, Google had 62.4 per cent of the worldwide online search market, and every time someone uses Google or one of its myriad services, Google collects more information about us.

Reed-Elsevier and its subsidiaries, such as Lexis-Nexis, have been doing something similar. Lexis-Nexis alone maintains billions of records, including media reports, legal documents, and public records collected from 36,000 sources around the world. In February 2008, Reed Elsevier, owner of the LexisNexis Group, announced that it was seeking to acquire commercial data broker ChoicePoint in a $4.1 billion deal would create a “global information-gathering powerhouse that would collect and analyse billions of records about who people are, where they live and with whom, and what they own”. With customers including government agencies, insurance companies, banks, rental apartments, corporate personnel offices and private investigators, both companies have played key roles in law enforcement, homeland security and intelligence.

In addition to the private sector, governments are also collecting and centralising their collection of personal data. The advent of electronic health records is one example. Law enforcement authorities and intelligence agencies are constructing vast biometric and DNA databases. (It is not yet known whether the December 2008 decision of the European Court of Human Rights that retention of innocent people’s DNA and fingerprint records by police is illegal will mean that the UK will scrap part of its DNA database or whether it will expand it to include all citizens.) The US Department of Homeland Security seems to have a voracious appetite for personal data, as it collects such data on every individual flying into or out of the United States.

557 Johnston, Philip, “Will the Government now take DNA from us all?”, The Telegraph, 4 Dec 2008. http://blogs.telegraph.co.uk/philip_johnston/blog/2008/12/04/will_the_government_now_take_dna_from_us_all
Undoubtedly these gigantic private sector enterprises and national security agencies will offer more personalised services and improve our safety and security, but the implications of these data concentrations are not as well explored or understood as they should be, but it is already clear that data concentrations create the risk of giant data breaches and losses, as shown by the sale of 21 million German bank account details reported in December 2008, the loss of 25 million child benefit records in the UK in October 2007, the illegal access of tens of millions of credit and debit card numbers through the systems of TJX, the US discount retailer, in 2006, or the theft of 92 million e-mail records from AOL in 2003. But the security or vulnerability of these databases is not the most important issue. Rather, the key issue is how the data aggregators use the information they already have at their fingertips. Function creep is inevitable. Control and manipulation of consumer-citizens does not seem far-fetched at all. The sociological implications also warrant analysis, notably in regard to the diminishing trust that citizens extend to political institutions.

7.2.4 Raising the awareness of and educating stakeholders

How can consumers be educated about the dangers of publishing location information about themselves, so that they can make informed choices about what location-based services to subscribe to, or with whom to share their current location (e.g., publishing it on their social networking site)?

Are consumers able to configure the disclosure policies of their personal positioning technology (and of any devices that they rent or borrow) so that it conforms to their interests?

How can consumers be educated about the implications of their online behaviour, in particular their online searches?

How will personal mobile storage affect personal data theft and corresponding crimes (e.g., fraud, blackmailing)? How can we effectively protect personal mobile data from third party access, even if the data are lost?

Many experts see problems in the consumers’ lack of awareness of the impact of the ways in which new information technologies can be used. Positioning systems have become very popular while most users are not aware that the systems not only provide information, but also are able to send information and receive responses such as adverts.

The public needs to be reminded over and over again that nothing is ever free. Those taking advantage of “free” online applications as an alternative to buying such software for use on their own personal computers may have to agree to the use of their data (perhaps aggregated) for “tailoring” other services (such as personalised advertising) by the operators.

There is also a challenge in raising the awareness of and educating the corporate sector, not only in Europe, but also abroad, specifically with regard to mechanisms for the international transfer of personal data, i.e., the Safe Harbour Agreement, binding corporate rules (BCRs) and contractual arrangements. The authors of a study carried out for the EC indicated that foreign-based companies had an imperfect understanding of the requirements of the Safe Harbour agreement, but the authors believed that these problems could be overcome by
providing better guidance on the mechanics as well as the meaning of the Safe Harbour data protection principles.\(^{558}\)

Airlines and travel agents are expected to provide passengers with information about the collection and transfer of their passenger name records. However, the Article 29 Working Party found that they were not doing so in a satisfactory way.\(^{559}\)

### 7.3 Profiling

#### 7.3.1 More personalised services = more data gathering and processing

In general, we can assume most consumers like personalised services. Probably they believe that personalised services mean they are being treated as an individual rather than as part of a depersonalised mass market. Personalisation of services comes at a cost. The more services are personalised, the more personal data are needed by the service provider. Indeed, some service providers have a voracious appetite for personal data. Their appetites are being abetted somewhat by data aggregators, who fuse data from multiple sources.

It is not just industry that is engaged in data mining and fusing data. Governments are in this game too, especially for containing terrorism and law enforcement. There are still many technical challenges to overcome in data fusion, but they have not deterred technologists.

Should there be legal requirements governing fusion of personal data? One can envisage the fusion of multiple position reports from different devices in order to derive detailed movement profiles. Location-based services are still in their infancy, yet they promise to significantly affect the citizen’s privacy through their potentially comprehensive location records assembled in the process of service provision.

IPTV is another example of a new application enabling the collection of personal data and profiling. With traditional broadcast television, it was not possible to know who was watching what except by asking consumers. However, with television distributed via the Internet, viewers can be identified by their IP address, so that it becomes possible to monitor who (at least which IP number) watched what, for how long and how often. This loss of anonymity creates socio-economic as well as socio-political challenges.

- One possible consequence is that the recorded data can be used to create user profiles. This could be used for personalised advertising according to what individual consumers like to watch.
- Another threat is that these data can be combined with other data, for example, from credit or consumer cards, which will contribute to making consumers increasingly transparent.

Among other examples mentioned in Chapters 2 – 6 of how new technologies lead to greater personalisation is smart metering, which can monitor in real-time the energy consumption of domestic appliances. The primary purpose of such smart meters might be to improve energy

---


efficiency, but the data collected from consumers could be used for other purposes, including discriminatory pricing, profiling and detecting habits and particular events (e.g., when others come to visit).

7.3.2 Search engines

Search engines, which have been described as “a gateway to the Information Society”\(^{560}\), target advertising at the user based on the search terms he or she uses. They log the user’s IP address and over time collect lots of data on the user’s interests.

Google is, of course, the pre-eminent search engine, and it collects more personal data than any of its competitors. In his new book about Google, Randall Stross says, “Google has also started collecting personal information about its users. If you so choose, Google stores your photos, videos, e-mail messages, calendar, word processing documents, spreadsheets, presentation slides, bookmarks to your favourite Web pages, online discussion groups, personal blog, instant messaging chats, social network messages, and stock portfolio. No category is too personal to be deemed unsuitable for Google’s organizing – one’s medical records can also be included, with the launch in May 2008 of Google Health. And Google’s reach extends right into the home: the files that sit on your personal computer can be indexed by Google software, if you give it permission to do so.”\(^{561}\)

The accumulation of such vast amounts of personal data raises numerous challenges to privacy and trust for Europeans. One key issue is the extent to which users are protected by European law from the use of personal data by Google and other search engines, the repurposing and security of those data.

In an opinion released in April 2008, the Article 29 Data Protection Working Party the Data Protection Directive does apply to the processing of personal data by search engines, even when their headquarters are outside the EEA. It said, “Search engine providers must delete or irreversibly anonymise personal data once they no longer serve the specified and legitimate purpose they were collected for and be capable of justifying retention and the longevity of cookies deployed at all times. The consent of the user must be sought for all planned cross-relation of user data and for user profile enrichment exercises. Website editor opt-outs must be respected by search engines and requests from users to update/refresh caches must be complied with immediately. The Working Party recalls the obligation of search engines to clearly inform the users upfront of all intended uses of their data and to respect their right to readily access, inspect or correct their personal data in accordance with Article 12 of the Data Protection Directive (95/46/EC).”\(^{562}\)


561 Stross, Randall, Planet Google, Free Press, New York, 2008. The Economist raised almost exactly the same concern and examples in an article pre-dating the Stross book by one year: “The big new fear is to do with the privacy of its users. Google’s business model assumes that people will entrust it with ever more information about their lives, to be stored in the company’s ‘cloud’ of remote computers. These data begin with the logs of a user’s searches (in effect, a record of his interests) and his responses to advertisements. Often they extend to the user’s e-mail, calendar, contacts, documents, spreadsheets, photos and videos. They could soon include even the user’s medical records and precise location (determined from his mobile phone).” The Economist, “Who’s afraid of Google”, 30 Aug 2007. http://www.economist.com/opinion/displayStory.cfm?Story_ID=9725272

Generally, search engine providers fail to provide an overview of the different purposes for which they process personal data.

Many Internet companies argue that a user enters into a de facto contractual relationship when using services offered on their website, such as a search form. Even if one accepted that argument, their processing of data may not meet the strict limitation of necessity as required in the Directive.

If personal data are stored, the retention period should be no longer than necessary for the specific purposes of the processing. Therefore, after the end of a search session, personal data could be deleted, and continued storage therefore needs an adequate justification. However, some search engine companies seem to retain data indefinitely, which is prohibited.

Search engines should make clear to users what information is collected about them and what it is used for.

The Article 29 Working Party drew various conclusions, among which was that “search engine providers must delete or anonymise (in an irreversible and efficient way) personal data once they are no longer necessary for the purpose for which they were collected.” It called upon search engines to develop appropriate anonymisation schemes. It also said it did “not see a basis for a retention period beyond 6 months.”

Google said, however, that it does not consider European law on data protection to be applicable to itself, even though Google has servers and establishments in Europe. It did, however, say it would reduce its data retention period to nine months (not six months as the Article 29 Working Party said). According to a 16 Sept 2008 press release, the Article 29 Working Party said, “Google refuses for the moment to submit to the European data protection law.”

7.4 SURVEILLANCE

Citizens are surveilled in many different ways, by video cameras, microphones, on the Internet. Their communications may also be monitored. On a per capita basis, UK residents are surveilled more than in any other country. It has frequently been noted that on average Londoners are photographed 300 times a day. Now the UK government is considering building a vast new database, at a cost of £12 billion, to monitor the e-mail, telephone and internet browsing records of every person in Britain. Currently, MI5 has to apply to the Home Secretary for warrants to intercept specific e-mail and website traffic but, under the new plan, Internet and mobile phone networks could be monitored live by GCHQ, the Government listening post.565

Apart from issues such as the security of such vast databases or the misuse and abuse of such data, the more fundamental question is: Is a surveillance society the kind of society we want? Do we want Big Brother watching us all time, wherever we are, whatever we are doing? At least in 1984, Winston Smith knew when and where Big Brother was watching, but the “new”

surveillance systems, so termed by MIT’s Gary Marx, are less visible and more continuous in time and space, provide fewer opportunities for targets to object to or to prevent the surveillance, are greater in analytical power, are disseminated faster and more widely, and are less expensive than the “old” surveillance techniques.

7.5 INFORMED CONSENT

There is wide consensus in the literature supporting the notion that it might be too easy to get apparently “informed” consent. If we want particular products or services, we may need to give our consent to service providers or product suppliers to do what they will with our data, at the expense of our privacy and perhaps even our dignity. Many consumers, especially young people, are judged as if they did not attribute much value to their privacy just because they seem to willingly give so much away on social networking websites and in many other ways, with apparently little or nothing in exchange.

Why is this happening? Do people perceive that they are getting greater value from using search engines or social networking websites than the value of their privacy? Are notions of privacy changing? Or is there a problem with attributing to consent the pivotal role it currently enjoys?

The issue of informed consent has been cropping up in many different contexts recently.

To use one example from section 7.2.1 above, when The Telegraph learned that the government was “floating” the idea of allowing medical researchers and pharmaceutical companies access to medical records without asking the consent of the person whose medical conditions the data records, it said “such a proposal, were it ever to become law, would be an outrageous infringement of every individual’s basic right to protect their privacy… Your records belong to you, and the Government is not entitled to use them without your permission.”

In the UK’s vast e-health scheme, the notion of “implied consent” has surfaced as an issue. According to one survey, as mentioned in section 3.2.4, 59 per cent of GPs were unwilling to upload any record without the patient’s specific consent and were increasingly concerned about the government’s plan to automatically upload the records of everyone who does not register an objection. Government ministers said unless someone objected, it would be assumed that they had given “implied consent”. However, this “implied consent” is at variance with the views of the Article 29 Working Party which has said that patients must give their explicit informed consent and that opt-out solutions do not meet the requirement of explicit consent.

Behavioural advertising raises a number of privacy challenges:

- Are consumers adequately informed that (when) their online behaviour is being monitored?


565 This “implied consent” is at variance with the Art 29 WP document referenced below wherein it says patients must give their explicit informed consent and that opt-out solutions do not meet the requirement of explicit consent.
• Do consumers have to opt out of such services or should they rather have the choice of opting in?
• How visible should monitoring companies make opt-in or opt-out information? Should notices to the consumer be “unavoidable”?\(^566\)
• What would constitute informed consent (opt-in) to participate in such services?
• If several members of a family use the same computer, is there a risk that younger members will be hit with offensive or inappropriate adverts based on the browsing habits of the adult user?
• Should the monitoring companies be required to make certain consumer disclosures in regard to this practice and, if so, what? For example, how the data are collected, used and protected?

The UK Department of Business, Enterprise and Regulatory Reform (BERR) said Phorm should be operated on the following basis:
• The user profiling occurs with the knowledge and agreement of the customer.
• Users will be presented with an unavoidable statement about the product and asked to exercise a choice about whether to be involved.
• Users will be able to easily access information on how to change their mind at any point and are free to opt in or out of the scheme.

Before a US Senate committee hearing on behavioural advertising, AT&T and Verizon, two of the largest service providers in the country, pledged not to track their customers’ web habits unless they obtained explicit consent. Verizon said that meant “meaningful, affirmative consent from consumers”. The crux of the debate in the Senate committee is whether consumers should have to opt in – or affirmatively consent – to be tracked or whether they should merely be given the opportunity to opt out of tracking if they don’t like the idea. Google, Microsoft and many other Web companies have espoused the opt-out model.\(^567\) Some companies argue that if users have to opt in, many would choose not to do so, which it turn could undermine the Internet economy because so much of what is presented on the Web is supported by advertising.

Much could be done to distinguish more clearly between genuine consent and consent that is simply enforced agreement.\(^568\)

It has been suggested that providing personal data as a condition of access to a site or an online service could be viewed not merely from the standpoint of data protection legislation but also from that of consumer law, in terms of unfair practices in obtaining consent\(^569\) or the major detriment arising from the imbalance between the value of the data secured and that of the services supplied.

---


Consent of minors requires special attention, especially, for example, in the context of their heavy participation in social networking (see section 3.3.1 above), the activities of which increasingly rely on location data (for instance, in mobile virtual communities). Moreover, the cases in which adult subscribers monitor minors represent a special challenge.

Another issue involving consent is that regarding cookies and whether users are adequately informed (if at all) about cookies and whether they agree to their use (in every case). Of course, users can adjust their browser settings so that cookies cannot be deposited on their computers, but some might argue that most users are hardly aware of their browser settings and the implications of those settings and, further, such settings could hardly be construed as informed consent to what happens to their data.

Similarly, we can assume, as the Article 29 Working Party has, that most Internet users are unaware of the large amounts of data that are processed about their search behaviour, and of the purposes for which they are being used. If they are not aware of this processing they are unable to make informed decisions about it.  

7.6 IDENTITY MANAGEMENT

Identity management can be seen both as a response and as a challenge. This depends strongly on the technical approach chosen to model an identity layer in the current Internet.

Current identity management consists of dozens and hundreds of separate accounts created at every website where the user wants to be known. Even though these accounts are held at separate entities and use freely chosen usernames (pseudonyms), they are often joined together by one and the same contact e-mail address. Furthermore, it is hard to keep track of the number of accounts created, as well as the information held (and its validity) in each of them.

Early attempts at simplifying online account management threatened to aggravate the problem, by trading in privacy for convenience: Instead of dozens of accounts and passwords, users would use a single central account with a single identity (often dubbed “Single Sign On”), which would then log them into the diversity of Web services they were using. Microsoft’s “Passport” scheme is probably the best known of those attempts, in which Microsoft was heavily critiqued for its centralised role in most, if not all, of their users’ communications involving Passport-enabled sites. Similar centralised proposals were made by other industry players and associations, such as Liberty Alliance. Another strong criticism involves the ability of participating websites to exchange information with other sites about customers through the shared single identity.

Since then, identity management solutions have moved to more decentralised architectures, which alleviates most of the privacy issues associated with a central identity provider.

---


However, challenges still remain regarding the security of such decentralised authentication, especially with respect to man-in-the-middle phishing attacks.

Identity management also plays a key role in e-government services, where future identity cards are envisioned to contain also a digital identity that can be used to access a variety of governmental services online. Securing such official online identifiers, especially in light of more administrative public functions being offered online, remains a key challenge in future governmental identity schemes.

### 7.7 Enforcing Existing Legislation

Some have questioned how well existing legislation is being applied, how existing legislation can be better enforced, whether incentives can be devised to encourage companies to comply with data protection principles, whether existing legislation is up to the task of dealing with new technologies, applications and services that were not foreseen when the legislation was introduced.


The EC has recognised some of the provisions in these Directives need to be updated. As mentioned elsewhere, on 13 November 2007, it introduced a proposal to amend Directive 2002/58/EC and on 24 September 2008, the European Parliament adopted a resolution supporting the Commission with, however, some amendments. The new legislation should strengthen provisions relating to breach notification, better protection against spam and malware, and better enforcement.

#### 7.7.1 Lacunae in Existing Regulation

One problem with the e-Privacy Directive is the limited scope of application of most of its provisions, limited to the supply of public electronic communication services in public networks.\(^{573}\) It does not take into account the increasing importance of private communication networks, nor the need to protect individuals from being monitored in such circumstances. Nor does it take into account the progressive blurring of public and private communications networks.

The Directive’s limitations have been underlined especially in reference to RFID. Despite the recent proposal to include an explicit reference to RFID in an amended e-Privacy Directive, RFID would still remain partially uncovered (i.e., RFID not connected to publicly available electronic communications services in public communications networks).

---

Identifying which actors should be considered relevant for the application of rules concerning data protection and privacy poses a special legal challenge. The Article 29 Data Protection Working Party has said that the definitions of “electronic communications services” and “to provide an electronic communications network” are not clear and give rise to several questions. Indeed, certain actors playing increasingly relevant roles in electronic communications are not providers of electronic communications services, but information service providers. Those actors, however, might be considered providers of electronic communications services when providing certain services.

It has been pointed out that applications such as social networking sites tend to blur the distinctions between service providers (“authors” or “editors”) and users/consumers (or “readers”).\textsuperscript{574} It remains to be determined whether the concept of controller as exists in the current European legal framework for data protection is still relevant and operational when end users are progressively becoming the main actors in the processing of personal data.

Today, using data mining and profiling techniques, one can obtain profiles of subjects without processing any data strictly related to an identified or identifiable person.\textsuperscript{575} Data used to build the profiles can simply relate to devices or even files accessed. However, the processing may be an interference with the individual’s private life, either because of the constant monitoring it requires, the consequences of the profiling or the decisions taken based on the profile obtained.

The main legal challenge in this context is how to avoid these practices taking place outside the scope of any provisions on privacy or data protection. Alleging that processing does not fall under the scope of data protection rules, those responsible sometimes tend to avoid complying with those rules.

Challenges raised by the processing of IP addresses could be intensified in the context of the introduction of new protocols such as IPv6, allegedly leading to increased risks of profiling of user activities on the Internet, as well as increased risks linked to security and confidentiality issues.

\section{7.7.2 Difficulties in enforcing legislation}

Article 10 of the Data Protection Directive establishes the information or transparency requirements for the processing to be considered fair. These requirements are increasingly difficult to apply and increasingly neglected or ignored. Social networking sites have been identified as especially problematic, as users tend not to be aware of all the data collected about them.

Article 4 of the e-Privacy Directive says that providers of publicly available electronic communications services must take appropriate technical and organisational measures to safeguard the security of their services. In practice, it appears that the enforcement of security obligations needs to be strengthened.


\textsuperscript{575} For the concerns of data protection authorities on the global proliferation of profiling practices, see International Working Group (IWG) on Data Protection in Telecommunications, \textit{Resolution on Privacy Protection and Search Engines}, 28\textsuperscript{th} Conference, 2-3 November 2006, London.
An examination of the role of the different actors responsible for privacy and data protection in a ubiquitous Information Society, as already suggested, could help clarify responsibilities for security. The responsibilities of providers of electronic communications services might need to be complemented by measures implemented by other actors (such as providers of social networking applications or other information society services).

Profiling and data mining are likely to grow, especially as targeted advertising and targeted services grow. So too will their impact on communications, especially mobile communications. These practices rely on massive collection and protection of data, which are not always considered personal data by those providing the services. The transparency of profiling and data mining practices represents a key legal challenge.

The Article 29 Working Party has underlined that Article 5 of the e-Privacy Directive imposes an obligation to ensure confidentiality of communications irrespective of the nature of the network and whether the communication crosses borders to non-EU member states. The recognition of this right, however, appears not to be clear enough regarding the duties and transparency obligations of the different providers potentially involved, especially in the context of the ubiquitous Information Society. This might lead to a lack of effective protection of the right to privacy of communications.

There might be a need to adapt provisions relating to telephony to VoIP, to protect webmail services (not only traditional e-mail) and, in general terms, to provide a regulatory framework able to tackle threats to privacy and the protection of personal data represented by foreseeable and unexpected technological developments.

7.7.3 Data security

Protecting personal data continues to be a formidable challenge as the number of data breaches and losses indicate. An October 2008 report from the UK All Party Parliamentary Group on Identity Fraud says that there has been a “vast” increase in cyber crime, where fraudsters use the Internet and e-mail to tap into existing accounts or to find out credit card details.576 However, not all data breaches are due to cybercrime. Some losses are due to negligence. Furthermore, the complexity of securing data is made more difficult when the processing of personal data is outsourced or shared with third parties. The centralisation of databases, for example, of identity cards, medical records, communications records and so on where thousands of people may have access to those databases also adds a layer of complexity to security.

Another factor in data security is the lack of transparency. There are suspicions that many breaches and losses, in both the public and private sectors, go unreported. There is a paucity of statistical data too which would enable comparisons to be made between different companies and organisations and between different sectors.

7.7.4 How to encourage data minimisation

Data minimisation is both a challenge and a response. Encouraging (or forcing) companies and organisations, including governments, to minimise the amount of personal data they collect and process is a challenge. Indeed, it is virtually antithetical to the notion of

personalising services, targeting users with personalised advertising, checking credit-worthiness, investigating criminal activity, deterring terrorists and much else. Equally, new services offered by social networks, such as Facebook, MySpace, Flickr, YouTube, Twitter, also work against this principle.

Data minimisation is also a response to minimise the threats to privacy, but given the counter trends mentioned in the previous paragraph, there must be doubts about how effectively this principle can be implemented.

How can we create an environment where data controllers and processors and developers of new products and services have internalised this principle?

How can we support the desire of people to engage in social discourse and disclose information about themselves, while ensuring that the data are limited in diffusion, deleted in due course and eventually forgotten?

7.7.5 Is there a need to regulate virtual worlds?

Some might say that it’s difficult enough to regulate the real world without the challenges of regulating a host of virtual worlds. In fact, there are two principal challenges associated with virtual worlds. One is the way the site operators manage the privacy and/or data protection of users. The other is the privacy challenges that arise within the virtual world itself. The snag for regulators, policy-makers and users (and the website operators too, for that matter) is that there is a convergence or an overlapping of the real and virtual worlds, as exemplified by the convertibility of Second Life’s Linden dollars and real world currency. Even so, this would not be a significant issue if it were not for the fact that there are millions of users with avatars in the virtual worlds and that the virtual worlds impinge upon the real world. Should a person’s avatar (digital representation) be entitled to the same privacy protections afforded to the person him- or herself? If there are regulatory controls (for example, over excessive violence or pornography) over online gaming and the content of films, how different is that from regulating what goes on in virtual worlds? Even if a case can be made for regulating virtual worlds, regulators are confronted by the art of the do-able and constraints upon their resources. Hence, industry self-regulation with some guidelines might be a better alternative, at least for the time being until users clamour more vociferously for stronger enforcement measures.

7.7.6 Regulation vs. self-regulation

Heretofore, the European regulatory framework has been based on five fundamental principles:

1. Regulation should be kept to a minimum.

577 “Can an action that takes place in Second Life be regulated by a court in the UK? The answer should be, why not?... the regulation of virtual worlds is not only possible, it is a reality. When signing up to a game or virtual environment, users must set up an account. This can be limited to users connecting from a range of national IP addresses, or the provider could make payment restrictions, i.e. you must have a bank account in X country in order to create the account. Such vetting of potential users serves to impose de facto regulation into the environment by tying users through End-User Licence Agreements (EULAs), payment methods, and even liability by potential identification through their Internet Service Provider.” Guadamuz, Andrés, “Back to the Future: Regulation of Virtual Worlds”, SCRIPT-ed, Vol. 4, Issue 3, Sept 2007. http://www.law.ed.ac.uk/ahrc/script-ed/vol4-3/editorial.asp
2. Regulation should be based on clearly defined policy objectives of:
   (a) fostering economic growth and competitiveness; and
   (b) ensuring that objectives of general interest are met where they are not satisfied by market forces alone.
3. Regulation should strike the right balance between flexibility and legal certainty.
4. Regulation should be technologically neutral or objectively justifiable if it is not.
5. Regulation may be agreed globally, regionally or nationally, but should be enforced as closely as is practicable to the activities being regulated.\(^{578}\)

Regulation and self-regulation are challenged by the advent of new technologies, products and services. For example:

- Should certain standards be set for monitoring consumer online behaviour?
- Should industry be encouraged (required) to self-regulate such practices? Or should the practice be subject to regulatory oversight?
- Are the actions of the companies engaged in behavioural advertising adequately monitored and especially with regard to how they use and reuse the data they have collected?

7.8 INTERNATIONAL TRANSFERS OF PERSONAL DATA AND GLOBAL REGULATION

The complexities of international transfers of personal data remain a potent and not adequately resolved issue.

Concerns have often been expressed about the difficulty of enforcing EU law on the transfer of personal data from the EU to third countries. Also as potentially problematic is the regulatory framework for television programming originating in third countries but at the disposition of European consumers whose consumption patterns can be tracked by those beyond European borders.

If European citizens opt to use Google Health or Microsoft Vault or other similar offerings, what conditions might the EU seek to impose? And how effective could such conditions be on companies based outside Europe?

Further empirical research is needed to assess how non-EU companies are using and protecting personal data from Europe, how procedurally easy or difficult it is for European consumers to have access to their data and to correct them if they are incorrect. Empirical research is needed with regard to the repurposing of data by the US government and industry. Further research is needed with regard how Europeans can determine who has their data.

As mentioned in Chapter 5 above on international transfers of personal data, more information and research is needed to better understand how well contractual arrangements, the Safe Harbour agreement and binding corporate rules are working, how well personal data are protected outside the EU and how well companies based outside the EU are implementing the procedures. So far, it appears that better guidance for those companies is needed.

Airlines and travel agents are expected to provide passengers with information about the collection and transfer of their PNRs. However, the Article 29 Working Party found that they were not doing so in a satisfactory way.

Still another issue to be resolved is making travellers aware, before they travel, that their electronic devices could be searched.

7.9 Trust

Trust and confidence underpin our society and economy. When trust and confidence plummet, as they have during the financial meltdown, the consequences are all too plain to see. The same holds true in the ubiquitous Information Society. Indeed, some challenges such as the implementation of e-government and e-commerce schemes go beyond the Information Society itself. The media have given lots of attention to data breaches and losses, to the development of new mega-schemes involving the collection of yet more personal data, which have contributed to the distinct loss of trust and confidence that government and industry can protect our data, that they will use the data for only the purposes for which they were originally collected, that new schemes are undertaken only after extensive public consultation and privacy impact assessments, that they are indeed justified.

Undoubtedly, there is an anomaly that social networking has skyrocketed, while at the same time public trust is so low. Yet the public has shown its disapproval in some schemes such as targeted advertising and some schemes such as Facebook’s Beacon “service” (informing your friends what you have purchased). Although Google is the most popular search engine, if it started doing something people don’t like, no doubt there would be a similar outcry and rebuilding public trust would take a long time.

As biometric identification systems become more widely deployed, there is a distinct risk of further erosions in trust if consumers are misidentified and consequently denied a service (e.g., boarding an airplane).

Many visions of a future smart environment rest on a personal trusted device that acts as a single trusted intermediary in unknown smart environments. How will trust be affected if these devices are as prone to attacks as today’s desktop PCs and laptops? And if they can be searched at border points?

One of the biggest challenges in implementing e-health concepts is gaining the public’s confidence that their electronic health records will be safe and secure. One survey in the UK found that three-quarters of those questioned thought medical records in the national e-health scheme would become less secure. Despite governmental assurances (which aren’t worth much in view of many data losses and data breaches), protecting medical privacy is more difficult today than just a few years ago for many reasons, not least of which is that more people have access to patient information and that patient information is more easily accessible when it is stored in digital form.

Michael Swaine has observed that “Trust is always important in business, but it is basic to all these Web 2.0 projects in a way that it wasn’t in earlier Internet businesses… most of Web 2.0 seems to be about the development of online communities… which depend wholly on user
contributions or build value from user ratings or recommendations… In probably all Web 2.0 businesses, but especially in media-centric ones, recommendations are a means of adding a layer of value to the interactions… Trust is the big issue for many Web 2.0 ventures.”

Although there have been many publications, articles and books written about trust, it seems there is still a need for more, especially about the dynamics of trust in different contexts involving regulation, self-regulation and technology-based privacy instruments.

7.10 ASSESSING HARM TO A PERSON’S PRIVACY

Empirical research is needed to assess the harms incurred by individuals from privacy losses, including the repurposing of their personal data.

One can assume there are psychological impacts when one’s life is exposed to others. There may also be physical or financial harms when malfactors try to take advantage of those whose personal information is exposed.

Some ID theft victims can spend thousands of dollars and months or years dealing with credit bureaus and debtors from accounts fraudulently opened in their names, but the law doesn't appear to take into account lost opportunities associated with identity theft. According to the US Federal Trade Commission, some consumers victimised by identity theft may lose out on job opportunities or be denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

Peter Hurst, chief executive of CIFAS, the UK’s fraud prevention service, said, “Identity fraud is serious, and no-one should be complacent about it. Quite apart from financial losses, the effect on victims can be very distressing. Where a victim’s identity has been seriously compromised, it can be an extremely time consuming and frustrating process to untangle the threads of deception.”

Even figures in the public domain, such as politicians, film stars, musicians and TV personalities, can be sufficiently stressed out by undue intrusions on their private lives that they have taken legal actions to penalise offenders.

It may be problematic to quantify stress and psychological upsets caused by harms to one’s privacy but that does not mean they are any less real than financial losses incurred as a result of identity theft.

7.11 BALANCING VALUES

Stakeholders are continuously balancing privacy against other values. Policy-makers and regulators are pulled in different directions, between the needs to balance personal data protection and encouraging economic growth, between privacy and surveillance. Consumer-citizens need to balance their sense of privacy and the attractions of social networking, the ease of buying online, downloading some new helpful applications, between paying for personal, desktop software, such as Microsoft Office, and getting similar applications free of charge from cloud computing operators, such as Google App. This tension will continue.

Our sense of privacy, however we define it, has surely changed over time. Most people seem more willing to expose more of their personal details than people did say 20 years ago before the advent of the World Wide Web. Even so, most people still have some sense of privacy; there are still aspects of their lives and identity that they do not want to give away.

Privacy advocates, data protection authorities, the Article 29 Data Protection Working Group and the European Data Protection Supervisor may not be regarded as helpful to industry which does not want to be burdened with having to inform consumers what they are doing with their personal data any more than law enforcement authorities, intelligence agencies or cyber criminals for that matter.

Balancing competing values and interests is a difficult task. Here are some examples:

- How should the location privacy of minors be balanced against the desire of parents to know where their children are? What about employees and employers? Can children and employees be forced to be locatable?

- How can we strike a balance between communication privacy and the need of law enforcement to observe and inspect communication patterns of suspects in VoIP systems?

- How can we balance the benefits of technologies such as reality mining and tracking applications with the privacy problems they raise?

The move toward e-health systems highlights another example of balancing competing values, for example, that which would allow researchers access to electronic health records. One could argue that people’s consent should be obtained first, but it could well be practically impossible to obtain everyone’s consent or even those with particular conditions which are the subject of the research. Furthermore, people being treated today have benefited from the research involving others in days gone by.

EHR pose many complexities in balancing competing values, as amply illustrated in a recent article in the Scientific American. If patients have too much control over their electronic health records, physicians will not have confidence in the accuracy or completeness of the records. In response, they will likely feel compelled to retake histories and order new tests, undermining the efficiencies of networks and adding cost to care. On the other hand, if patients have too little control, many may engage in defensive steps such as opting out of networks, paying cash for off-record services or declining certain care altogether. With the increasing availability of individual genetic maps, some employers may justifiably not want to recruit prospective employers who cannot or should not function in high risk areas (e.g., an electric power company would not want to hire someone who is prone to seizures to fix wires
at the tops of utility poles). EHR create major challenges in deciding which individuals and entities have a right to which information and for what purposes.\textsuperscript{582}

Other new technologies, such as social tagging, involve balancing competing values. Social tagging can be viewed as a democratic phenomenon where anyone can make pithy comments about anything on the Web, but critics worry about misuses. Users can make anonymous comments, which protects their privacy, but some users can take advantage of the anonymity to make malicious social tags which can harm other users and undermine trust. The result highlights some dissonance between privacy and trust, i.e., anonymity can protect privacy, but undermine trust. Wikipedia encountered a similar problem with bogus, inaccurate and intentionally misleading entries.

Some areas such as public safety, defence, state security, the activities of the state in the area of criminal laws and the economic well-being of the state fall outside the scope of data protection legislation, yet there are well-justified fears that our privacy and personal data may be abused in precisely these areas.

http://www.sciam.com/article.cfm?id=tougher-laws-needed-to-protect
8 POSSIBLE RESPONSES

In Chapters 2 to 6, we identified specific challenges as well as specific possible responses to those challenges. In the previous chapter, Chapter 7, we summarised the key challenges in a more generic, higher level way. In this chapter, we summarise some of the principal responses and their utility.

Generally, we are of the view that responses should be incentive-driven, i.e., that stakeholders have incentives to “do the right thing” in addressing the challenges. For example, an EC trust seal might be seen as something service providers will want to have on their home pages because it gives them credibility with consumers, but to be granted a trust seal, they need to take certain privacy-protecting measures. Similarly, if the EC funds development of privacy-enhancing technologies through its Framework Programme, industry is likely to want to invest some time and effort into responding to calls for proposals and making sure that any technologies developed are marketable.

Legislation and regulation are usually only effective to the extent that they can be enforced. It may not be possible to catch everyone guilty of abusing the market, but at least enough have to be caught and penalised so that one can assume, rightly or wrongly, that the legislation or regulation is working and that it is having a deterrent effect. Otherwise, the unenforceability of legislation risks further undermining public trust and confidence. In this regard, determining which responses (e.g., regulation vs self-regulation) are viable is a tricky business.

The responses to the challenges to privacy and trust described in this chapter can be undertaken by the European Commission as well as other stakeholders, including the Member States, the data protection authorities, industry, the media, civil society organisations, academia and individuals. In Chapter 8 on Instruments, we refer more specifically to the instruments at the disposition of the European Commission that can be used to initiate some of the responses described in this chapter.

We need to point out the distinction between responses and instruments. When we refer to responses, we refer to specific responses to specific challenges. One can characterise those responses, as we have done, as technical, administrative, legal or whatever. The Commission (and other stakeholders) have the means (instruments) to implement those responses. Thus, a response to a challenge might be to bring in a new regulation. That regulatory response is a manifestation of an instrument at the disposition of the Commission, i.e., its ability to develop regulations. An instrument is a tool, is a means for doing something. The something done is the response. The EU’s ability to make regulation, its regulatory power, is the instrument, while the regulation actually made is the response.

The boundaries between some of the responses referenced in the following sections are fuzzy. Privacy seals, for instance, cover multiple aspects of privacy enhancing responses: They are raising the consumer’s awareness that a product or service has been certified as providing a certain level of privacy protection. For this purpose, the product or service has to undergo a

---

583 How effective the deterrent is also depends on whether the penalties imposed are seen to be proportionate to the offence. In the UK, ICO has said that existing penalties have not halted the unlawful trade in confidential personal information, consequently it has recommended stiffer penalties, including imprisonment of up to a maximum of two years for all those individuals and businesses obtaining, supplying or buying personal information illegally.
well-defined and transparent privacy impact assessment, which should be based on a commonly agreed set of criteria. These criteria may be the outcome of an open working group with the involvement of all stakeholders. For our analysis, we have classified responses according to their primary purpose. We assess the responses in more detail in sections 10.3 and 10.4.

8.1 TECHNICAL RESPONSES

In the following sections, we present a few of the most relevant privacy enhancing technologies (PETs). We group possible technical responses into six areas, in each of which there is a need for further research.

8.1.1 Privacy-compliant data management

At the core of any comprehensive solution must be an information storage concept that is able to process data in compliance with the collection policies under which the information was obtained. Such an infrastructure forms the basis for providing any higher-order services such as compliance verification and auditing, online subject access (see section Error! Reference source not found. below), or anonymisation.

Agrawal et al. coined the term Hippocratic databases for such systems,\(^{584}\) in which data and processing policies are inseparable units, and all processing is done in full compliance with the individual data element’s policies. This general concept has also been extended to explicitly support auditing processes\(^{585}\) and to deter data piracy through watermarking.\(^{586}\) Casassa Mont et al. have coined the term “sticky policies”\(^{587}\) for such systems, which aim at establishing trustworthy computing environments with respect to privacy. The goal is to build computers that cannot process personal data in any way other than that expressed in a policy attached to it, which is enforced with the help of policy-based data processors running on an underlying trusted computing platform.

8.1.2 Development tools and libraries for privacy-compliant data handling

In order to promote the use of privacy-compliant information processing, developers need easy access to a variety of tools and libraries that support them in designing, creating and maintaining data processing applications. Similar to ready-to-use security libraries today, information systems of the future must come with well-documented and easy-to-configure privacy tools, e.g., for enabling and querying auditing, or to adjust company-wide privacy policies without affecting previously collected information.


As a result of many years’ research, the technical community has developed and made available a core of powerful, well understood, cryptographic technology.\(^{588}\) It offers building blocks from which secure mechanisms can be built for a very wide range of applications. The main ones are:

- symmetric encryption
- message authentication codes
- public-key encryption
- digital signatures
- one-way hash functions
- random number generation
- zero-knowledge protocols.

So far, similar ready-to-use privacy tools and libraries are missing, resulting in a lack of privacy-compliant mechanisms being integrated and deployed into new systems. In order to increase the commercial uptake of such techniques, privacy-modules must ship with most modern database distributions and libraries.

### 8.1.3 Supervisory tools for inspection and verification

Based on the core information processing modules, both companies and supervisory bodies need end-user tools to control and verify the particular data processing practices in place. These might include both local and remote access modes, e.g., in order to allow data protection agencies to conduct spot audits from their own offices.

Several commercial systems for privacy audit support have been implemented. Two popular ones are Tivoli Privacy Manager from IBM and Openview Select from HP.

The *Tivoli Privacy Manager*\(^ {589}\) offers policy enforcement mechanisms for business databases and systems, which help corporate privacy officers manage information privacy. Basically, the software supports the abstraction of privacy and data-handling rules from applications and IT systems, based on existing policies and individual consent. Furthermore, the privacy manager monitors access to personal information and generates detailed audit logs and automatic compliance reports.

The *HP Openview Select*\(^ {590}\) family and business software offers privacy and identity management support in data lifecycle management. At the core of the system lies the concept of “privacy obligation” policies, which are policies dictating expectations and duties on how these data should be handled in accordance with privacy preferences and guidelines. Privacy obligations introduce the need to deal with privacy-aware information life cycle management, i.e., ensuring that the creation, storage, modification and deletion of data are driven by privacy criteria.


\(^{590}\) For more on HP Openview Select, see: [http://www.hpl.hp.com/personal/Marco_Casassa_Mont/Projects/PrivacyAwareIdentityLifecycleManagement/PrivacyAwareIdentityLifecyclemanagement.htm](http://www.hpl.hp.com/personal/Marco_Casassa_Mont/Projects/PrivacyAwareIdentityLifecycleManagement/PrivacyAwareIdentityLifecyclemanagement.htm)
Further techniques are the use of audit trails and agents, database audit interfaces, log files and steganographic technologies.

### 8.1.4 Infrastructural support for anonymous communication

In order to eliminate out-of-band disclosures of information whenever communicating with a particular service, users (data subjects) must be able to rely on a communication infrastructure that can ensure their anonymity. For example, a sophisticated certificate-based authentication system that uses zero-knowledge techniques to allow users anonymised or pseudonymised access to a service will be less effective if all communication can be traced back to a fixed residential IP address that will uniquely identify a subscriber. This does not imply that all communication must be anonymous, but only that it must be sufficiently easy and cost-effective to use anonymous communication whenever needed.

Notable recent developments have resulted in information-hiding technologies to produce privacy-supporting protocols, such as anonymous credentials\(^{591}\) by Camenisch and van Hereweghen, which are used in identity management tools, or the *Eternity Service*\(^{592}\) proposed by Ross Anderson which represents reliable, redundant, distributed storage of information while hiding ownership of data.

Infrastructural support also includes security guarantees at the system level, i.e., an execution environment that can offer data subjects the necessary integrity of their data and interaction software. The use of trusted computing hardware\(^{593}\) might allow critical communication systems to ensure the absence of malicious code that could log keystrokes or reroute data.

A set of services offers re-routed, anonymous or encrypted access to the Web, the Internet or e-mail. The underlying technology is known as a “Mix”, a set of computers that work together to hide the original sender of a message or request. Instead of sending a request or message directly, participating clients send it to another Mix computer, which strips out all sender information and passes it on to another, random Mix participant. After several such forwards, one Mix computer finally forwards the message to the final destination. Any reply is then routed back along the entire chain of computers until it finally reaches the original sender. One of the earliest such services is Anonymizer.com, though it represents only a single “Mix” (i.e., a proxy) and thus represents a single point of attack, e.g., for a subpoena.

Closely related are unobservability tools, which make access to services or data “invisible”. Usually, such tools protect one or more communicating partners from being observed by someone else. In the following paragraphs, we present a few relevant tools based on Mix technologies.

*MixMaster*\(^{594}\) is an anonymous remailer, a program that provides protection against traffic analysis and allows a user to send e-mail anonymously or pseudonymously. For e-mail and

---


\(^{594}\) MixMaster: https://mixmaster.sourceforge.net/
other communication, simple encryption is not enough, as the sender and recipient are still observable.

The AN.ON\textsuperscript{595} (“Anonymität Online”) project, together with its client JAP (“Java anonymous proxy”) is a joint research and development project for unobservable Internet surfing. Instead of connecting directly to a web server, users take a detour, connecting with encryption through several intermediaries. JAP uses a predefined sequence of linked Mixes, i.e., a Mix cascade. Since many users use these intermediaries at the same time, the Internet connection of any single user is hidden among the connections of all other users. This solution provides perfect anonymity, as no one, not even the provider or the intermediary service, can determine which connection belongs to which user. Linking a connection to a user is only possible if all the intermediaries work together to sabotage the anonymisation. AN.ON and JAP are carried out at the Technical University Dresden and the Independent Center for Protection of Privacy in Kiel. JAP was also turned into a commercial product (JonDo) in the scope of the new commercial service JonDonym.

The TOR\textsuperscript{596} project was initiated as “Onion Routing” (OR) by the United States Office of naval research and comprises projects researching, designing, building and analysing anonymous communications systems. Its Firefox plug-in, TORPARK, is an excellent example of usability for PET systems. It provides a browser button to turn on anonymity, and a button to flush (i.e., re-randomise) the TOR connection. Even unskilled users can just run it and surf anonymously. Thanks to its success, the product turned commercial in 2007, under the name of XeroBank.\textsuperscript{597} xB Machine\textsuperscript{598}, also a XeroBank product, is advertised by the firm as “the most secure operating system in the world”, touting excellent usability.

In the context of anonymous communication, of special relevance are anonymous or pseudonymous payments, such as electronic cash (application of the “blind signature” technique) or prepaid solutions (e.g., PaySafeCard\textsuperscript{599}).

Privacy and PET usage in collaboration platforms and within Web 2.0 communities are research fields that need further investigation. Kohlweiss et al. propose using newer cryptographic protocols to protect privacy and to hide location information in geo-spatial, mobile applications.\textsuperscript{600} In the context of location data in mobile phone networks, a notable development is Geopriv\textsuperscript{601}, a large geo-spatial privacy framework.

8.1.5 Identity management tools

Identity management tools assist the user with managing his or her online identity. Such support does not imply that users would actively need to manage their identity – ideally, these would operate in the background and simply appear as data management repositories from

\textsuperscript{595} AN.ON – Anonymity.Online: http://anon.inf.tu-dresden.de/
\textsuperscript{596} TOR: http://www.torproject.org/
\textsuperscript{597} XeroBank: http://xerobank.com/
\textsuperscript{598} xB_Machine: http://xerobank.com/xB_Machine.php
\textsuperscript{599} PaySafeCard: http://www.paysafecard.com/
which the user would select data to share or in which updates and corrections could be made. Their operations would, however, effectively decouple the individual actions of data subjects between different services as much as possible, creating separate pseudonymous identities as needed.

At a larger scale, such identity management tools also entail various secondary functions that could be under the control of the user, though an automated operation would be preferred: cookie management, data privacy filters, certificate repositories, etc. According to the data protection principle of data minimisation, identity management should rely on transmission and processing of the minimum amount of identification data needed for a particular purpose.

An example for such an underlying anonymous communication infrastructure is IDEMIX (which stands for “Identity Mixer”) developed by IBM Research. IDEMIX is a system for strong anonymous or pseudonymous credentials and comprises a set of libraries of cryptographic protocols and data formats. IDEMIX aims to attest identity information using zero-knowledge protocols, which keep the identity secret but accomplish attestation of the desired property (e.g., that a person has a driver’s licence and is over 25 years old). The EU-funded FP6 PRIME project (Privacy and Identity Management for Europe) has built a wide variety of identity management systems and services on top of IDEMIX. It also explored social, legal and economic aspects of identity management. The PRIME work is continuing in the FP7 project “PrimeLife.”

Liberty Alliance is an example of an industry-driven identity management approach. The Liberty Alliance comprises 30 organisations and aims to establish open standards, guidelines and best practices for federated identity management. The group was formed as an answer to the now discontinued Microsoft passport service, which planned to provide centralised user management. By now a successful venture, Liberty Alliance has been adopted by major system integration firms and suppliers. Similar efforts are Microsoft’s CardSpace, which is integrated into its Vista operating system, and the OpenID technology, which is already supported by a number of online services such as MySpace and Dopplr. Ann Cavoukian, the Privacy Commissioner of Ontario, Canada, has coined the term “transformative technologies” for such systems. Adoption of such services, however, is slow, as they lack the critical mass of supported services and sites that would allow consumers to rely on a single such identity service only. With few users to sign up, sites in turn are not in a hurry to implement support for these authentication standards. It is also important to note that these commercial efforts typically have a much smaller scope than the comprehensive identity management visions of, e.g., PRIME or PrimeLife. These services might form a first step to a more comprehensive solution though.

---

602 Privacy and Identity Management for Europe (PRIME): [https://www.prime-project.eu/](https://www.prime-project.eu/)
604 Liberty Alliance: [http://www.projectliberty.org/](http://www.projectliberty.org/)
605 See [http://netfx3.com/content/WindowsCardspaceHome.aspx](http://netfx3.com/content/WindowsCardspaceHome.aspx)
606 See [http://openid.net/](http://openid.net/)
608 Cavoukian sees transformative technologies as addressing common trade-offs between privacy and security, in particular in surveillance applications. Her examples include video surveillance software that automatically blurs or even removes faces or entire persons from a video stream, saving the information in a separate, encrypted file that can only be decrypted by the proper authorities following proper procedures.
Peyton et al.\textsuperscript{609} propose an audit trail service to enhance privacy compliance in federated identity management and describe a specific implementation conforming to the Liberty Alliance data service format. The solution protects the user's identity and provides a consolidated view of the data sharing activities associated with personal information.

Taking a broader view on identity management, many other end-user privacy tools exist. For example, privacy search engines\textsuperscript{610} that search for websites and online vendors that comply with one's personal privacy preferences have been investigated. Many tools that search for spyware on local computers, block it and suppress advertisements have been developed, both freeware and commercially, and are now integrated by major browsers, anti-virus software vendors and Microsoft (in the Malicious Software Protection system).

\textit{Cookie Cooker}\textsuperscript{611} is a tool that manages user profiles along with their set of browser-specific cookies. It enables users to assign distinct sets of cookies to their own “profiles”, which can then be activated, e.g., before shopping on-line. To mess up the server profiles, Cookie Cooker offers to swap cookies with other users, and offers advertising blocking. The ultimate goals are unlinkability and unobservability, by blocking advertisements, exchanging cookies between users, managing web identities, providing surf anonymity and protecting privacy (random form filling, storing data in encrypted files, etc).

With the spread of blogging, services are taking shape that will search the Web for information about a person and deliver a paid-for dossier. Deng et al.\textsuperscript{612} proposed a model for privacy infrastructures, to find and track relevant images and videos captured by, for example, other people on the street using their camera phones, and distributed on the Web. The authors make use of digital rights management techniques and data identification techniques such as digital watermarking (embedding information into a digital signal such as audio files, pictures or videos) and robust perceptual hashing (also known as fingerprinting).

The greater the information required by a PET, the higher is the risk of invading the privacy of individuals, although its value in trust enhancement could be higher. It is important therefore to know the scope of the PET to determine whether it is a trust-enhancing or an information-exploitation instrument.\textsuperscript{613} Usability, economic costs and legal impacts are also crucial factors when it comes to identity management, as these factors can significantly hinder adoption.\textsuperscript{614}


\textsuperscript{610} \url{http://www.worldprivacyforum.org/searchengineprivacytips.html}

\textsuperscript{611} \url{http://www.cookiecooker.de/}


8.1.6 Online subject access tools

Closely related to identity management is the need for providing easy-to-use tools that support the right to subject access. Article 12 of Directive 1995/46/EC sets forth a legal right to “subject access” to personal data. With today’s prevalence of online services, offering data subjects an immediate online access to the information that data controllers have on them would greatly simplify the subjects’ means to exercise their access rights.

In many cases, this might simply be integrating remote data management systems for the various service providers a user interacts with. However, services that offer pseudonymous or even anonymous use might still collect and maintain a user profile for the (unidentified) data subject – this might for example be the clickstream data collected under the user’s IP address. In such cases, a more comprehensive solution is needed that would support secondary authentication methods, as the user’s identity is not yet associated with the pseudonymous data.

Also, the right to data correction and deletion might conflict with audit requirements. Similar conflicts might arise from data attributed to several data subjects. Technical solutions to these challenges must take legal implications into account.

8.1.7 Anticipating new technologies and their impacts

A technical meta-response might be the early anticipation of technologies that might significantly affect privacy and trust. Foreseeing new technologies and analysing their implications is a difficult task, but one worth undertaking anyway to forestall, if possible, consequences injurious to individual privacy.

The Commission could usefully undertake or sponsor research specifically aimed at identifying new technologies that could have deleterious impacts on privacy. Note that this is closely related to (and indeed overlaps with) technology assessments in general, e.g., recent Commission activities surrounding RFID technology, or the work by the Swiss Office for Technology Assessment (TA-SWISS) on Pervasive Computing.

8.2 Administrative responses and measures

Administrative measures are essential to respond to the challenges posed by the deployment of ubiquitous computing technologies, because they can reach all phases from R&D to deployment. Administrative measures and responses should aim for an integration or fair balance of the interests of all stakeholders. The possible domains of such measures and responses can be separated in three layers: first, direct responses and actions of public administrations, which are covered in this section; second, public authorities can initiate measures to create public awareness (see section 8.3 below) and, third, enforcement and regulation of co-operation between producers and consumers (see sections 8.4 and 8.5). Within all three levels, governments, industry associations, consumer rights groups and other civil society organisations can play an important role for the benefit of all affected groups.

615 See http://www.rfidconsultation.eu/
8.2.1 Evaluation of privacy aspects of ICT research proposals

Government support for new technologies should be linked more closely to an assessment of technological consequences. In view of the far-reaching social effects that new ubiquitous Information Society technologies have (or are likely to have), there has been a deficit in this area, a point made by one of the partners in our consortium a few years ago, which is still a valid observation.  

Research and development (at least publicly supported R&D) should highlight future opportunities certainly, but also possible risks to society. The European RTD efforts constitute a very good opportunity to accomplish these goals and the European Commission has recognised that “privacy by design” should be an inherent part of its RTD programmes. As a result the EDPS is assisting the European Commission in the evaluation process of proposals, in particular regarding possible data protection issues these proposals might trigger. Although researchers are inclined to underestimate privacy risks, every research project should commit itself to explore possible risks in terms of privacy, security and trust, develop a strategy to cover problematic issues and involve users in this process as early as possible. The “PRISE” project recently developed such criteria for data protection compliant and privacy enhancing security which took into account the OECD privacy principles, which are referenced below as an example of a voluntary code of conduct as well as the work on Privacy Impact Assessments in different countries. The EDPS considers these criteria as a good basis for evaluation of research proposals.

8.2.2 Standards

Standards form an important administrative response to the challenges to privacy and trust posed by the ubiquitous Information Society. Administrations should comply with standards themselves and should ensure other organisations, private and public, do so as well.

With so much of our personal data flowing outside the EU, when we “agree” to use Google or social networking websites or virtual worlds such as Second Life or any of a myriad of other websites or services, which will only increase with the Internet of things, ambient intelligence, ubiquitous networking or however one chooses to describe the ubiquitous Information Society, with the biometric requirements of travel from one country to another, with the exchanges of personal data between government for security and other purposes, the controls and safeguards offered individuals by the Data Protection Directive are stretched very thinly indeed.

The European Union should renew its push for international privacy standards, especially through the International Organization for Standardization (ISO). The 29th International Data Protection and Privacy Commissioners’ Conference held in Montreal in 2007 adopted a Resolution expressing support for the development of “effective and universally accepted international privacy standards”. It said it would make available to ISO its expertise for the development of such standards.

The ISO has at least achieved consensus on four components of privacy within the ISO/IEC 15408 standard on evaluation criteria for IT security, as follows:

- **Anonymity** ensures that a subject may use a resource or service without disclosing its user identity.
- **Pseudonymity** ensures that a user may use a resource or service without disclosing its identity, but can still be accountable for that use.
- **Unlinkability** ensures that a user may make multiple uses of resources or services without others being able to link these uses together.
- **Unobservability** ensures that a user may use a resource or service without others, especially third parties, being able to observe that the resource or service is being used.

Another ISO standard relevant to privacy is ISO 17799 [now renumbered to 27002], the code of practice for information security management, which was first published in 2000 and updated in July 2005. Since then, an increasing number of organisations worldwide formulate their security management systems according to this standard. It provides a set of recommendations for information security management, focusing on the protection of information as an asset. It adopts a broad perspective that covers most aspects of information systems security.

---

http://www.privacyconference2008.org/index.php?page_id=142. The 30th Conference decided to establish a working group to draft a proposal for setting international standards on privacy and personal data protection, which will be submitted to the 31st conference. Among other things, the proposal would formulate the essential guarantees for better and flexible international transfers of data.


625 Similar standards and guidelines have also been published by other EU Member States: The British standard BS7799 was the basis for the ISO 17999 standard. Another is the German IT Security Handbook (BSI 1992).
Among its recommendations for organisational security, ISO 17799 states that “the use of personal or privately owned information processing facilities ... for processing business information, may introduce new vulnerabilities and necessary controls should be identified and implemented.”\textsuperscript{626} By implementing such controls, organisations can, at the same time, achieve a measure of both organisational security and personal data protection.

ISO 17799 acknowledges the importance of legislative requirements, such as legislation on data protection and privacy of personal information and on intellectual property rights, for providing a “good starting point for implementing information security”.\textsuperscript{627}

ISO 17799 is an important standard, but it could be described better as a framework or code of practice rather than a standard addressing the specificities of appropriate technologies or how those technologies should function or be used. Also, ISO 17799 was constructed against the backdrop of today’s technologies. Hence, the adequacy of this standard in a ubiquitous Information Society needs to be considered.

A related standard is ISO/IEC 27001:2005 which specifies the requirements for a documented information security management system within the context of an organisation’s overall business risks. It is designed to ensure the selection of adequate and proportionate security controls to protect information assets and give confidence to interested parties. Among other things, it is intended to be used within organisations to ensure compliance with laws and regulations, by internal and external auditors to determine compliance with policies, directives and standards, and by organisations to provide relevant information about information security to customers.

With the creation of Working Group 5 (Identity Management and Privacy Technologies) within Sub-Committee 27 (Information Technology Security)\textsuperscript{628}, the ISO signalled its intention to push ahead with the development of privacy-related standards. The Working Group issued a call for liaison to the International Conference of Data Protection and Privacy Commissioners, noting specifically “mutual interests in the area of data protection and privacy within both organizations and the Working Group's goal to harmonize aspects for identity management, biometrics and privacy in the context of information technology with a set of international standards”.\textsuperscript{629}

Standards currently under development by the new ISO Working Group include ISO 29101 – A Privacy Reference Architecture (best practices for consistent technical implementation of privacy principles); ISO 29100 – A Privacy Framework (defining privacy requirements for processing of personal information in any information system in any jurisdiction); and ISO 24760 – A Framework for Identity Management (framework for secure, reliable and privacy compliant management of identity information).

One difficulty with standards is that it can take a long time to develop and agree something that is acceptable to the world community.

\textsuperscript{626} ISO/IEC 17799:2005, p. 11
\textsuperscript{627} ISO/IEC 17799:2005, p. ix.
\textsuperscript{628} JTC 1/SC 27 IT Security techniques
8.2.3 Open working groups

Open working groups can sometimes become de facto grassroots standards organisations. An example of one which is gathering momentum is the DataPortability Project, which promotes the idea that individuals should have control over their data by determining how such data can be used and who can use them.\footnote{630} According to its website, the DataPortability Project maintains:

- You should be able to decide what you do with those data and how they get used by others.
- Open source solutions are preferred to closed source proprietary solutions.
- Bottom-up distributed solutions are preferred to top-down centralised solutions.

The DataPortability Project promotes the use of existing standards that enable data portability, identifies new standards required to fulfil the data portability vision and makes the output of the DataPortability project freely available.

The DataPortability Project is open to anyone, individuals, companies and organisations, and aims to reach resolution by consensus and to have transparency in decisions.

DataPortability is an effort by a group of volunteers and Internet application vendors. Founded in November 2007, the project has gained support from several major Web industry players including Google, Facebook, LinkedIn, Flickr, Twitter, Digg and Microsoft.\footnote{631}

Another open standard working group (sort of) is OpenID, which is a shared identity service, allowing Internet users to log on to many different websites using a single digital identity, eliminating the need for a different user name and password for each site. OpenID is a decentralised, free and open standard that lets users control the amount of personal information they provide.\footnote{632}

An OpenID is based on use of a URL, which can be the domain name of the individual’s own website, or the URL of an OpenID identity provider. When the user logs in with an OpenID, he or she has to log in to an identity provider for validation.

Using OpenID-enabled sites, web users do not need to remember traditional items of identity such as username and password. Instead, they only need to be registered with any OpenID identity provider. Since OpenID is decentralised, any website can use OpenID as a way for users to sign in. OpenID does not require a centralised authority to confirm a user’s digital identity.

OpenID has been adopted by many large Internet players, including AOL, BBC, Google, IBM, Microsoft, MySpace, Orange, VeriSign and Yahoo! acting as providers.

A European counterpart, the OpenID Europe Foundation headquartered in Paris, was founded in June 2007. It is a non-profit organisation promoting and deploying the OpenID software framework in Europe.

\footnote{630}{http://wiki.dataportability.org/display/dpmain/Home}
\footnote{631}{http://en.wikipedia.org/wiki/DataPortability}
\footnote{632}{http://openid.net}
As of July 2007, there were reportedly more than 120 million OpenIDs on the Internet while about 4,500 sites had integrated OpenID consumer support.

OpenID is decentralised in the sense that

- Users can host their own identity on any server they choose, without having to ask anybody for permission or approval. They can also choose to have it hosted by one of the increasingly many OpenID hosting services.
- Service providers can choose from a variety of software implementations from a variety of vendors and Open Source projects.
- “OpenID does not crumble if any one company turns evil or goes out of business.”
- The OpenID specifications are developed in an unencumbered, meritocratic process, which is open to participation by anyone.
- Anybody can use their own technical innovations within the OpenID framework, even if they replicate, or compete, with the OpenID specifications themselves.633

OpenID has, however, suffered some criticism with regard to security vulnerabilities, such as phishing.634 Writing in The New York Times, Randall Stross, also a professor of business at San Jose State University635, argues that we need a log-on system that relies on cryptography, not mnemonics. He favours replacing passwords with so-called information cards, icons on the computer screen that we select with a click to log on to a website. The click starts a handshake between machines that relies on hard-to-crack cryptographic code. This is what the Information Card Foundation, supported by Google, Microsoft and PayPal, among others, proposes. However, that solution too has been criticised:636 “Everything running directly on a PC (specially with MS-Software) can be faked or spied on,” says Rick Smith, author of the Cryptosmith computer security blog. “The only thing which helps is an external ID (Card or USB-Dongle) with embedded microprocessor which handles all the communication with embedded cryptography and refuses to be spied on.”

8.2.4 Public procurement

Though it should be self-evident that ICT systems procured by state authorities should be compliant with existing data and privacy protection regulations, this is not always the case – especially when selection criteria strongly emphasise economically advantageous offers. Thus, in the procurement of ICT products, more emphasis should be given to critical issues such as privacy, security and trustworthiness. As in other advanced fields, it will be a major challenge to develop a sustainable procurement policy that can cope with ever-decreasing innovation cycles. The focus should not be on the characteristics of an individual product or component, but on the systems into which components are integrated.

Moreover, public procurement programs can be an effective means to initiate research and development of improved products and services in terms of security and privacy or identity protection. If the state acts as a buyer of strategically important innovative products and

635 Stross is also author several books, most recently Planet Google, Free Press, New York, 2008.
services, it contributes to the creation of the critical demand that enables suppliers to reduce their business risk and realise spill-over effects.\textsuperscript{637}

Finally, it is important to pay attention to the secondary and tertiary impacts resulting from deployment of large technical systems such as those that characterise a ubiquitous Information Society (e.g., electronic health records, national ID schemes, biometric passports, etc.). An evaluation of the indirect impacts is especially recommended for larger (infrastructure) investments and public services.

\textbf{8.2.5 Testing third-country data protection safeguards}

In view of the ease with which personal data can be transferred from the EU to third countries, the efficiency and effectiveness of third-country data protection safeguards (for example, in the context of the Safe Harbour agreement) should be tested periodically, e.g., to check how easy or difficult and time-consuming and costly it is for individuals to determine who outside the EU has their information, to verify its accuracy, to correct it if it is wrong, to know how their data are being used, protected and/or shared. The Commission and/or EU Member States’ data protection authorities could do this proactively or wait until they receive complaints from individuals. The former course of action will probably cost more, but could avoid unpleasant surprises downstream when safeguards are discovered to be weak or non-existent and costs and delays to the individual unacceptable. The latter course of action would cost less, but risks adverse publicity, a straining of relations between EU and third-country regulators and a loss of confidence by citizens in EU-negotiated agreements and EU data protection authorities’ ability to protect individuals.

\textbf{8.2.6 Audits and more resources for DPAs}

Unannounced visits by data protection authorities to companies and government departments processing personal data are necessary to ensure regulation and enforcement actions are meaningful. Not every organisation can be audited, of course, because data protection authorities and information commissioners simply do not have the resources, although given the scale of problem of abuses of personal data and failures in protecting such data adequately, they could obviously rise better to the job before them if they had more resources and powers to audit.

Audits are useful to see how well (or badly) existing legislation and regulation are being enforced and whether their provisions are working as intended. Despite Article 5(3) of Directive 2002/58/EC, it seems that anyone connected to the Internet can find hundreds of cookies on their computer about which they were never informed. Even if the user clicks his agreement to the terms and conditions of certain applications, the specificities of the purpose of particular cookies is not usually provided.

Audits are also necessary to verify how well industry self-regulation and codes of practice are working and whether personal data are being used for secondary purposes, that is, for purposes which were not specified when the data were originally collected. Audits can be

useful in determining whether the collection of personal data leads to discriminatory practices, for example, by the introduction of new technologies for insurance purposes.

Unfortunately, many data protection authorities do not have the powers or resources they need. In the UK Data Sharing Review Report, the co-authors (one of whom was Richard Thomas, the Information Commissioner) said “A strong regulator is also needed… [with] sufficiently robust powers and sanctions available to it; and… resourced adequately… with a power to impose financial penalties for wilful and reckless breach of the data protection principles… We also believe that stronger inspection and audit powers are required”.

The Commission has made similar observations. “One concern is respect for the requirement that data protection supervisory authorities act in complete independence and are endowed with sufficient powers and resources to exercise their tasks. These authorities are key building blocks in the system of protection conceived by the Directive, and any failure to ensure their independence and powers has a wide-ranging negative impact on the enforcement of the data protection legislation.”

Thus, the effectiveness of this response measure depends upon adequately resourced and empowered data protection authorities.

8.2.7 Benchmarking, metrics and additional research

Just how useful various measures are in responding to privacy and data protection challenges will usually require some benchmarks. As already mentioned, we need some way of measuring how successful privacy protection is or has been, some metrics that would address, for example, the following:

- How many enforcement actions have been taken by data protection authorities?
- How many successful prosecutions have there been?
- How much have offenders been fined or otherwise penalised?
- From what sectors have offenders come?
- What initiatives have data protection authorities taken to inform the public (data subjects) and data controllers about the arcana of data protection law?
- Is citizen awareness of privacy issues and how personal data can be protected improving?

Section 3.6 on cybercrime said that some statistical and comparative data could have a salutary effect in fighting identity theft and strengthening the resolve of institutions to better protect personal data. Heretofore, consumers, regulators and businesses have lacked objective tools to compare the incidence of identity theft across financial and other institutions targeted by fraudsters. Without such tools, consumers cannot “vote with their feet” and choose safer institutions, regulators cannot allocate oversight and enforcement resources to high-risk institutions and practices, and businesses themselves cannot assess how well they perform.


[640] For example, as mentioned in section 3.2.4 on e-health above, in the first three years after the US Health Insurance Portability and Accountability Act (HIPAA) regulations went into force, thousands of complaints alleging violations have resulted in just two criminal prosecutions, no civil fines and many agreements to fix problems that may have occurred without any penalty.
relative to competitors in fighting this crime. While competition is a powerful force for consumer protection, the lack of information about identity theft makes the market less effective in creating a race to the top among institutions to shield consumers from fraud.\textsuperscript{641}

Beyond the utility of metrics, further research is necessary to investigate how new technologies and applications are being used. For example, it would be useful for the EC, Member States and/or academia to do some research on what third-party developers of applications for social networking websites are doing with the data they collect (and not only social networks, other websites too; Mozilla Firefox, a popular web browser, has hundreds of third-party-developed applications or add-ons).

\section*{8.3 Awareness-raising and education measures}

It is obvious that public education and awareness-raising campaigns are necessary to encourage citizens to take steps to increase the security of their personal data in view of the results of a recent Eurobarometer survey where only a minority (22 per cent) of Internet users said they used tools and technologies that increased data security on the net, i.e., firewalls or cookie filtering.\textsuperscript{642}

Awareness-raising actions are constantly needed, to provide information about the rules applicable, the roles of all stakeholders, their rights, obligations and liabilities, to make them known and understood. This point of view is nowadays shared and supported by many public institutions, including the OECD, which has said that “all participants in the new information society …need… a greater awareness and understanding of security issues and the need to develop a ‘culture of security’.”\textsuperscript{643} To reach this aim of a “culture of security”, the initiation and support of awareness-raising actions is only the first step, which could also lead to a “culture of fear”. The second step consists of various actions to educate all stakeholders, not only consumers, about the rules, procedures, rights and obligations as well as about the remaining risks and possible safeguards. Measures to create awareness about the rules and procedures, the risks and possible safeguards can also contribute to addressing concerns that undermine trust and confidence.

\subsection*{8.3.1 Media attention, publicity and public opinion}

One of the most effective responses to privacy threats and lapses in personal data protection, trust and confidence is media attention which often and successfully shows its power in whipping up public opinion.

Media attention comes in different forms. The most obvious is that of the mass media, with stories in the press and broadcast media.

\begin{flushright} 
\end{flushright}
The sustained coverage of privacy issues, identity theft and losses of personal data by the news media, especially influential newspapers such as The New York Times and Washington Post in the US and their counterparts in Europe, such as The Guardian, The Financial Times, Le Monde, El Mundo and El País, have made an impact. The UK government is regularly harassed by the media when personal data are lost, especially since the loss of 25 million child benefit records in October 2007. Similarly, The New York Times and Washington Post regularly snipe at the US government (and American industry) on warrantless eavesdropping and other privacy threats.

Personalised advertising or behavioural marketing has been the subject of extensive media scrutiny in the US and UK in 2007 and 2008. Undoubtedly unwelcome media attention was a factor in several Internet companies in the US deciding to abandon plans to trial NebuAd’s deep-packet inspection technology for targeted advertising. Jeffrey Chester, executive director of the Center for Digital Democracy, said that NebuAd “seriously underestimated the privacy concerns”.

Social networking sites have also been sensitive to media attention, of which they have received rather a lot. Facebook’s retreat on its Beacon service is another case in point.

Another increasingly influential medium is the blogosphere. Some bloggers have gained rather extensive followings, and policy-makers and industry sometimes find themselves at the pointed end of barbs by bloggers such as Michael Arrington (TechCrunch), Rick Smith (Cryptosmith), Cory Doctorow (Boing-Boing), Bruce Schneier (Crypto-Gram), Tim O’Reilly, (the O’Reilly Radar), Richard MacManus (ReadWriteWeb) and so on.

Cultural artefacts, such as films and novels, may serve as safeguards against the threats and vulnerabilities posed by advanced technologies, including ambient intelligence. Science fiction in particular often presents a dystopian view of the future where technology is used to manipulate or control people, thus, in so doing, such artefacts raise our awareness and serve as warnings against privacy-invasive technologies. An example of a cultural artefact is Stephen Spielberg’s 2002 film, Minority Report, which depicted a future embedded with biometrics and ambient intelligence and which served to convey messages or warnings from the director to his audience. Minority Report is by no means unique as a cultural artefact warning about how future technologies are like a double-edged knife that cuts both ways, with advantages and disadvantages.

8.3.2 Sharing best practices

The European Commission could publish a study on examples of best practices, and the associated economic benefits to be gained from adequate data protection and/or the costs of breaches. Another way would be to have some contest or competition for the best security or privacy-enhancing product or service of the year. The US government’s Department of Homeland Security sponsors such competitions, and Europe could usefully draw on their experience to hold similar competitions in Europe.

---


To some extent this is happening. As an example, the Data Protection Agency for the Region of Madrid makes an annual award for best practice in European public services. It encourages organisations in the public sector to seek recognition for good data protection practices by applying for a prestigious European award which aims to increase awareness of best practice in data protection around Europe. In 2006, the award was presented to the projects “Providing confidentiality and Information Management and Technology Security Service to the United Kingdom NHS organisations across the South and West Yorkshire” and “Data Protection Plan 2005-2006 of the City of Madrid.”

In the US, the Federal Trade Commission won a similar award, the HP/IAPP Privacy Innovation Award for excellence in protecting personally identifiable information. The annual award is sponsored by Hewlett-Packard and the world’s largest association of privacy professionals, the International Association of Privacy Professionals (IAPP).

The UK’s Financial Services Authority has published examples of good practice that could help firms benchmark their own systems and make necessary improvements.

As an important example of best practice, the UK Data Sharing Review Report’s second recommendation says that “companies should review at least annually their systems of internal controls over using and sharing personal information; and they should report to shareholders that they have done so.” Such practice would also help to improve accountability.

Not only are there awards for best practice in data protection, there are also “awards” bad practices, and they too can have a good effect. For example, every year, Privacy International and a growing number of affiliate human rights groups present the Big Brother Awards to government agencies, private companies and individuals who have excelled in the violation of our privacy. The juries worldwide consist of lawyers, academics, consultants, journalists and civil rights activists.

Section 3.2 on e-insurance above referred to a Big Brother Award to the German company ptv, a developer of on-board units (OBU) for “Pay-as-you-drive” (PAYD) systems, which can be used by insurance companies to collect data on driver behaviour for differential pricing of premiums. After being given this “award”, the company started to develop new technological

---


648 Federal Trade Commission, “FTC Earns 2008 Privacy Innovation Award”, Press release, 23 Sept 2008. http://www.ftc.gov/opa/2008/09/privacyaward.shtm. In its press release, the FTC noted that more than 30 federal agencies have requested copies of its materials on privacy protection and that Americans surveyed by the Poneman Institute rated the FTC as one of the most-trusted federal agencies for privacy protection.


651 http://www.bigbrotherawards.org/
solutions, where the collected data are aggregated within the OBU, so that the creation of movement patterns or the use for law enforcement is no longer possible.\textsuperscript{652}

In short, “naming and shaming” can have as salutary effect on bad data protection practices as awards for good practices.

\textbf{8.3.3 Public education and awareness raising}

IT and design courses are now widely part of school curricula at secondary, if not primary levels. In view of the wide use of the Internet and heavy use of social networks by young people, privacy and personal data protection should be at the heart of IT courses. As mentioned above in section 3.3, parents and teachers have important roles to play in ensuring children are aware of the risks of posting personal data on the Internet. The aforementioned survey conducted by ICO, which showed that almost 60 per cent of 14-21 year olds said they did not realise that the information they were putting online could be permanently linked to them, provides evidence of the need for better education of school-age children.

The European Commission has begun supporting initiatives to raise public awareness of the potential risks children and young people can encounter online. One such initiative is INSafe, a network of national nodes that co-ordinate Internet safety awareness in Europe.\textsuperscript{653} The network was set up and co-funded within the framework of the European Commission’s Safer Internet plus Programme\textsuperscript{654}, which deals with new online technologies, including mobile and broadband content, online games, peer-to-peer file transfer, and all forms of real-time communications such as chat rooms and instant messages, primarily with the aim of improving the protection of children and minors. The programme has four main aims:

1. Fighting against illegal content
2. Tackling unwanted and harmful content
3. Promoting a safer environment
4. Awareness-raising.

These and similar initiatives are helpful in encouraging people to take better care of their personal data and to be cautious online. They should be supported further by the Commission, Member States and other stakeholders. The initiative of local educational authorities in London mentioned in section 3.3 is a particularly good one since it does not focus only on the Internet but a variety of new technologies. As we move toward the ubiquitous Information Society when things become embedded with intelligence, educational programmes should already be providing the public, including school children, with more information about embedded technologies too and possible risks they may pose to one’s privacy and personal data.

Formal educational programmes can be considered a form of awareness-raising. Less formal but no less valuable is the advice which the media, privacy advocacy organisations and governmental data protection authorities provide to citizens on steps they can take to protect their privacy and personal data.

See the following as a few among many examples:

\textsuperscript{653} http://www.saferinternet.org/ww/en/pub/insafe/about.htm
\textsuperscript{654} http://ec.europa.eu/information_society/activities/sip/programme/index_en.htm
• Rosen, Nick, “Living off the grid – how to escape the spies all around us”, *The Times*, 9 Feb 2008. http://www.timesonline.co.uk/tol/news/uk/article3338076.ece

In the US, the government has established various public awareness websites such as the Internet Crime Complaint Center (IC3)\(^655\) and It looks too good to be true\(^656\) (the latter is a joint government-industry initiative).

While such advice can be useful, the snag is that the threats to privacy and data protection from new ubiquitous technologies are constantly changing, so much so that some advice is virtually out of date by the time it is given.

### 8.3.4 Privacy and trust seals

Trust marks and trust seals can also be useful safeguards because they alert consumers and other individuals to an organisation’s practices and procedures through participation in a program that has an easy-to-recognise symbol or seal. In theory, they should foster public credibility and confidence.

Trust marks and seals are a form of guarantee provided by an independent organisation that maintains a list of trustworthy companies that have been audited and certified for compliance with some industry-wide accepted or standardised best practice in collecting personal or sensitive data. Once these conditions are met, they are allowed to display a trust seal logo or label that customers can easily recognise.\(^657\)

Such a trust mark must implement mechanisms necessary to maintain objectivity and build legitimacy with consumers. Trust seals and trust marks are, however, voluntary efforts, not legally binding, and effective enforcement needs carefully designed procedures and the backing of an independent and powerful organisation that has the confidence of all affected parties.

An example of a trust mark is the Kitemark® which, according to the British Standards Institution (BSI), has served as a mark of quality, integrity and trust for products since it was registered in 1903. The mark is also available for trade, professions and public services, and provides an independent third party endorsement that a service consistently meets the

\(^{655}\) http://www.ic3.gov
\(^{656}\) http://www.lookstoogoodtobetrue.com
requirements of the appropriate standards. Service providers need to have in place a quality plan or quality management system (e.g., ISO9001) and be evaluated against specific service criteria as set down in the standard. If successful, the company earns the right to use the Kitemark® in conjunction with its service. To maintain this right, BSI carries out regular inspections against the standard.658

Trust seals and trust marks are often promoted by industry, as opposed to consumer-interest groups. For example, Facebook has said it is setting up a Facebook Verification program for applications that meet the basic criteria of being secure and trustworthy. These applications will get added visibility and a graphical “badge”.659 Nevertheless, concerns remain that consumers’ desires for stringent privacy protections may be compromised in the interest of industry’s desire for the new currency of information. Moreover, empirical evidence indicates that even some eight years after the introduction of the first trust marks and trust seals in Internet commerce, citizens know little about them and none of the existing seals has reached a high degree of familiarity among customers.660 Though this does not necessarily mean that trust marks are not an adequate safeguard for improving privacy in ubiquitous computing environment, it suggests that voluntary activities like self-regulation have – apart from being well designed – to be complemented by other legally enforceable measures.661 One possibility for such measures could be the co-funding by administrative institutions, as happens with health-related websites, where the Commission co-funds the development of a set of quality criteria (“webseals”). Its aim is to increase transparency among health-related websites in the interest of serious service providers and users, ranging from citizens to health professionals.662

Some groups have suggested that any networked device, particularly those used by consumer-citizens, should come with a privacy warning much like the warnings on tobacco products.663 The prospect of such warnings catching on with industry, however, seems rather slender. A privacy seal with better prospects could be that which emerges from an EC-supported project, called EuroPriSe (the acronym for European Privacy Seal), which aims to introduce a trans-European privacy seal issued by independent third parties certifying compliance of IT-products and services with European regulations on privacy and data security. A EuroPriSe

658 http://www.bsi-global.com/en/ProductServices/About-Kitemark/Kitemark-for-services/
660 LaRose, Robert, and Nora Rifon, “Your privacy is assured - of being disturbed: websites with and without privacy seals”, New Media and Society, Vol. 8, No. 6, 2006, pp. 1009 - 1029.
fact sheet notes that citizens and business often need “a good faith belief” when using privacy relevant IT products and services, but that currently there is no transparent guidance for choosing a data security and privacy compliant product.

If it catches on664, the European privacy seal would help foster consumer protection and trust and provide a marketing incentive to manufacturers and vendors for privacy relevant goods and services. EuroPriSe is adapting the privacy seal (Guetersiegel) certification scheme used in the German state of Schleswig-Holstein. Indeed, the Schleswig-Holstein Independent Centre for Privacy Protection leads the EuroPriSe consortium.665

The Swiss have also developed a scheme for certifying data processing procedures. Under its Ordinance on Data Protection Certification (DPCO) of 28 September 2007 (it came into force on 1 January 2008), the Swiss Federal Council authorised the Federal Data Protection and Information Commissioner to issue guidelines on the minimum requirements for any data protection management system to be certified. The Ordinance says the Commissioner “shall take account of international standards relating to the construction, operation, monitoring and improvement of management systems, and in particular the standards ISO 9001:2000 and ISO 27001: 2005”. The Commissioner set out the guidelines in July 2008.666

Article 5 of the Ordinance says products may be certified if their primary purpose relates to the processing of personal data or their use results in the generation of personal data. Article 6 says that the certification of a data protection management system is valid for three years and that the certification organisation must conduct an annual summary review of whether the

664 According to an e-mail from EuroPriSe in Oct 2008, the project had “18 pilots from 10 countries (applications from January/February 2008). More than 50 international small, medium and large companies have expressed their interest since March. Not all of them offer products/services fit for certification. However, we know of another 10 companies who have actually started the evaluation process outside the pilot. Since January 2008, we have admitted approx. 60 experts who qualified to conduct evaluations. More than 50 people are on a waiting list for the next expert workshop after the project phase. This includes people from very well known firms.”
665 The €1,239,000 project began in June 2007 and finishes in November 2008. The other partners include the Agencia de Protección de Datos de la Comunidad de Madrid, the Commission Nationale de l’Informatique et de Libertés (CNIL), the Austrian Academy of Science, London Metropolitan University, Borking Consultancy (Netherlands), Ernst and Young AB (Sweden), TÜV Informationstechnik GmbH (Germany), and VaF s.r.o. (Slovakia). For more information, see www.european-privacy-seal.eu/
666 Guidelines on the minimum requirements for the data protection management system (certification of organisation or procedure according to article 4 DPCO) of 16 July 2008. See also the Ordinance to the Federal Act on Data Protection (OFADP) of 14 June 1993 (Status as at 1 January 2008).
requirements for certification continue to be fulfilled. The certification of a product is valid for two years and a product must be certified again if any fundamental changes are made to it.

Certification of personal data products or procedures is also possible in France, at least there is a legal provision for it. Under the French law on informatics and liberties, Article 11 spells out the mission of the Commission nationale de l’informatique (CNIL), the data protection authority. Article 11 3° (c) says that at the request of professional organisations or institutions, CNIL can produce a label indicating that specified products or procedures conform to legal requirements for protection of personal data. However, it seems this particular provision has yet to be implemented.

Another type of mark is that developed by the US Commerce Department’s International Trade Administration (ITA) for use on the websites of companies to signify that they have self-certified compliance with the provisions of the Safe Harbour agreement and to “illustrate their commitment to ensuring that EU citizens’ data is secure”, as the ITA assures us. The efficacy of actual implementation of privacy seals, at least in the US, has been questioned. A recent study found that “the websites that seek to publicize their concern for consumer privacy by displaying privacy seals were actually more likely to infringe upon their visitors’ privacy, at least in terms of the amount of personal information that they requested from consumers. Aside from a greater tendency to deposit cookies, the unsealed sites were no more likely than the sealed ones to infringe users’ physical privacy. Thus naïve consumers who view seals as a form of privacy protection may be disappointed.” However, the authors of this study offer several suggestions for overcoming existing shortcomings: The seal programs might improve their utility for the consumer by standardizing the ways in which the information is presented. For example, advertising and distracting graphics might be banished from pages containing privacy statements. Terms might be standardized and a glossary offered by the seal authorities. The content and sequence of sections of privacy statements might be further specified.

8.4 SELF-REGULATION AND OTHER MEASURES

While governments can play an active role in adopting legislation, promulgating guidelines or initiating education programmes, their role in self-regulation can be characterised as supportive of measures (nominally) initiated by industry to avoid the heavier hand of
regulation. The advantages of such measures are that they can supplement governmental measures such as research guidelines and codes of conducts and that they can be agreed and put in place faster than measures that need to go through several bureaucratic hoops. Governments and regulators often prefer self-regulation to legislation that may be difficult to enforce. However, self-regulation can be problematic in creating unbalanced, asymmetric solutions which may not adequately address the perceived problem or which may delay or sideline more appropriate solutions such as standardisation.

8.4.1 Codes of conduct

The OECD has helped government and industry in developing codes of conduct with its *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, adopted on 23 September 1980 and the more recent *Guidelines for the Security of Information Systems and Networks*.672 The latter were adopted as a Recommendation of the OECD Council in July 2002. In November 2003, the OECD published a 392-page volume entitled *Privacy Online: OECD Guidance on Policy and Practice*, which contains specific policy and practical guidance to assist governments, businesses and individuals in promoting privacy protection online at national and international levels.

Codes of conduct, as dodgy as they may be in some cases (i.e., they are ignored or are inadequate or not implemented in full), enjoy a large measure of public support. Recent research has shown that nearly half of all Internet users would support a voluntary code of conduct for bloggers and online commentators.673

Codes of conduct can have a salutary effect. When Google applied to join the Network Advertising Initiative, a trade group that sets standards for companies that collect data for use in targeting advertising, it was obliged to respect one of the core principles of the group, i.e., that its members provide “clear and conspicuous notice” of how they collect and use data. This has been interpreted to mean that a link to a website’s privacy policy should be on its home page.674 Until then, Google didn’t make reference to its privacy policy on its home page, but now (in a small font) does so.

Codes of conduct can sometimes be mixed with other measures as is the case with the recently introduced UK Council for Child Internet Safety, which reports directly to the Prime Minister and which monitors the Web for offensive content accessible by children. The Council has drawn up a voluntary code of conduct, under which websites can promise to root out violent or pornographic content within a set deadline and be vigilant in preventing bullying on message boards, but it can order that sites illegally encouraging suicide or harmful behaviour be taken down. The Council intends to introduce trust seals for software that it plans to have packaged with every computer sold for home use in the UK which will give parents controls limiting their children’s access to adult websites. The Council is also planning to push major search engines, such as Google and Yahoo, to make it easier for parents to limit what results are given in response to searches made by their children.675

672 http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html
8.4.2 Industry initiatives

Before announcing its new services, Phorm had Ernst & Young and 80/20 Thinking Ltd assess its system’s privacy features. This was a good move by Phorm. Not only does it have the benefit of (somewhat) undercutting possible opposition to a new service, but also it has genuine value for companies when they develop a new product or service to which they suspect there may be some opposition. This “preview-review” by reputable, independent third-party organisations (especially a privacy advocacy organisation) will help the company in seeing whether they have any “chinks in their armour”, any aspect that they have not addressed. If the company genuinely believes in the efficacy of its product or service, such a review by independent third parties will help them determine whether there are any privacy-enhancing improvements that could be made to their product before releasing it to the public. It also helps the company to build bridges with those from whom it might suspect of otherwise providing the most vociferous opposition. Such a tactic also has the value for the company of potentially increasing consumer trust and confidence in a new offering because it has been reviewed by an independent third party whom the consumer is more likely to trust than the company.

Similarly, Facebook and other social networks collaborated in a task force organised by the UK Home Office to establish guidelines on good practice, security and privacy for social networking websites. Facebook, it seems, has taken to keeping an increasingly watchful eye on its social network site in view of the surge in spamming that has begun to afflict its site (and others like it). It has been removing users that exhibit any suspicious activity. This might be an instance of good corporate behaviour that goes too far in the direction of social responsibility to the extent that some innocent users may be black-listed.

Cynics might argue that self-interest is clearly high in many such industry initiatives (or responses), but even so industry can show regulators that they are aware of and sensitive to public concerns and are willing to address them, as industry-leader Microsoft appears to have done in August 2008 when it confirmed that it is building new privacy-enhancing features into the eighth edition of Internet Explorer.

IE 8 program manager Andy Zeigler said in a blog that “Users should be in control of their information. That’s at the core of privacy. Privacy has two aspects: disclosure and choice. Disclosure means informing users in plain language about the data collected about them and how it’s used. Choice means putting users in control of their data and giving them tools to protect it.”

IE8 will include a feature called InPrivate Browsing which will let users control whether IE 8 saves their browsing history, cookies and other Internet data. Another feature, called InPrivate Blocking, will inform users about sites that can track their browsing history, and will allow them to block such activity. InPrivate Subscriptions will let users choose which websites to

---


subscribe to or block, while a fourth feature, Delete Browsing History, gives users control over their browsing history after visiting a website. All of these features already exist to some extent, but if Microsoft gives them more prominence and visibility and makes them more user-friendly, other browsers and industry players may follow suit. Good industry initiatives will have a ripple effect.

Indeed, that may already be happening. A few days after the Microsoft announcement, Google launched Chrome, a new browser competitor to IE, which enables Web-based applications that forego the need for applications installed on local PCs. Among Chrome’s new features is a special privacy mode that lets users create an “incognito” window where “nothing that occurs in that window is ever logged on your computer”, according to a Google promotional guide.

8.4.3 Training staff

Most companies and government departments could do a better job of protecting and securing personal data. Many simply do not take the risks of theft or loss sufficiently seriously. Section 3.6 on cybercrime mentions a survey of US and British businesses published in December 2007 by Kroll On-track, which found that fewer than half of the businesses in both countries had a strategy or policy in place on how to deal with electronically stored information. An important part of developing a serious strategy (preferably based on the ISO 17799 standard) is training staff (and preferably all staff) on good practice in protecting data.

Following the numerous and much publicised losses of data by the UK government in 2007 and 2008, all civil servants are to be regularly trained in data handling and protection. In addition, all staff will have to assess what information should be sent to them, either by post or e-mail, through “privacy impact assessments”. Security roles are to be standardised across Whitehall to ensure that someone is clearly responsible for data handling in each office.

The UK Data Sharing Review Report’s makes a couple of good recommendations germane to training: “All organisations routinely using and sharing personal information should review and enhance the training that they give to their staff on how they should handle such information.” [Recommendation 4] “As a matter of good practice, all organisations handling or sharing significant amounts of personal information should clarify in their corporate governance arrangements where ownership and accountability lie for the handling of personal information.” [Recommendation 2]

---


8.4.4 Individual initiatives and consumer actions

Consumers, en masse, can vote with their feet. They can object to too much advertising by deserting their social network sites – at least, that’s the theory. In January 2008, Deloitte warned in its annual predictions report of the potential dangers of the over-commercialisation of social networking websites.681

The power of individual consumers may be limited in fighting unfair corporate practices in collecting and processing personal data, but consumer organisations and other civil society organisations can give them greater leverage. CSOs can play a useful role as a mediator between service providers and individual consumers and, more particularly, in forcing the development of service contracts (whether real or implicit) between the service provider and the individual consumer that better protect the consumer’s personal data and how they are used. Consumer organisations can leverage their negotiating position through the use of the media or other means of communication with their members. CSOs could position themselves closer to the industry vanguard represented in European technology platforms and, possibly, industry associations by becoming members of such platforms and associations. Within these platforms, CSOs could encourage industry to develop “best practices” in terms of provision of services to consumers.

Individual initiatives can also have powerful consequences. An Internet user in the US, fed up with seeing so many unwelcome adverts appearing on his computer, took the initiative to develop the AdBlock program (as mentioned earlier), which blocks ads from appearing on the computer screen. Such software, made freely available on the Web, has alarmed companies who have said that undermining web ads will undermine the viability of the Internet itself. While undoubtedly an overblown claim, this claim nevertheless points to unintended consequences, where measures aimed at fixing one problem may create another, the so-called risk-risk phenomenon.

8.4.5 Transparency and trust-enhancing responses

It has often been said that trust is easy to destroy and difficult to rebuild (or words to that effect).

One of the biggest challenges in implementing e-services is gaining the public’s confidence that personal data will be safe and secure.

Like many e-services, protecting medical privacy is more difficult today than just a few years ago for many reasons:

- More patient information is collected, both in volume and in types of information.
- More people have access to patient information, including medical caregivers, researchers, and administrators in the health care system and, in many cases, employers and government agencies outside it.
- Patient information is more easily accessible because it is increasingly stored in digital form (and so it can be transmitted more easily than in paper form).
- Patient information is held for very long periods of time, and the longer it remains in existence, the greater the opportunities for abuse.

• More patient information is being collected by types and in volumes that are intended to aid medical practitioners in predicting future medical conditions with greater accuracy.

• Patient information (such as DNA information) is being (or soon will be) collected that has relevance to individuals related to the patient (parents, siblings, current and future offspring), thus raising the potential for significant violations of medical privacy and complicating both the technical and ethical issues involved in managing such information.682

Policy-makers in government and decision-makers in industry must be conscious all the time of the fragility of trust and be thinking about what they can do to earn the consumer-citizen’s trust. Transparency and engaging the public (for example, in consultations) are no guarantees of success in earning trust, but their absence greatly diminishes the prospects and nourishes suspicion. Sony might have avoided all the flak it got on its use of DRMs on its CDs and DVDs if it had been more transparent about what it was up to and why or, even better, engaged in a public consultation itself before it initiated the practice. If it had conducted a privacy impact assessment, along the lines of the UK guidelines, that too might have drawn attention to the risk it was taking on.

Trying to shift the blame for failures in the protection of personal data is not usually viewed as a trust-enhancing response, rather it is more like a surefire recipe for destroying confidence, as exemplified by the following press report: “The attempt by ministers to blame the loss of personal data on 25 million people on junior officials at HM Revenue & Customs (HMRC) was undermined… by scathing reports on the incident by two independent inquiries. They said the ‘entirely avoidable’ loss of two computer discs containing child benefit records on seven million families was due to ‘serious institutional deficiencies’ at HMRC and criticised senior management for not explaining data protection rules to junior staff.”683 By attempting to shift the blame, the UK government only dug a deeper hole for itself.

The key element in building or regaining trust is transparency. Indeed, some of have observed that much of the debate about privacy revolves around transparency. Hence, government, industry and any other stakeholder collecting or processing personal data should be transparent about what they are doing, what data are collected, how they are used and what controls are in place to protect the data from breaches or other loss. Transparency is so much better than being caught out and vilified by the media and suffering a consequent loss of trust by the consumer-citizen.

8.5 LEGAL RESPONSES

The eventual need for the introduction of new legislative proposals requires especially detailed scrutiny. EU legislative action is justified not only in terms of its general necessity for legislation in the specific field (as a “last resort” option), but also in terms of subsidiarity and proportionality. According to the subsidiarity principle, the EU may only legislate when action by Member States is insufficient. By virtue of the proportionality principle, the EU


may only act to the extent needed.

Legal responses supporting privacy and trust must also contribute to other aims such as the development of new technologies, the promotion of competition, the protection of consumers and the protection of the general interest.\textsuperscript{684} The legislative process preceding the adoption of any EC legal instruments is crucial to ensure that all aspects of the responses envisaged are duly taken into account in their eventual deployment. The legislative process allows for the integration of different stakeholders’ concerns, as well as the eventual redefinition of the response for better implementation.

This section presents a series of legal responses that are considered a priori convenient for the assurance of privacy and trust in the ubiquitous Information Society. They have been classified into three categories, based on their different rationales: (1) the protection of personal data, (2) ensuring the effectiveness of the right to privacy and (3) protecting privacy by taking into account the technological dimension of practices. This classification, inspired by relevant legal analysis,\textsuperscript{685} avoids a reduction of possible legal responses to the challenges to privacy and trust in the ubiquitous Information Society to legal developments of the right to personal data protection.

Indeed, even if data protection legislation can be conceptualised as a “first line of defence” for the individual,\textsuperscript{686} there is no reason to exclude or handicap the EU-level development of complementary approaches, which provides different layers of protection. On the contrary, an explicit recognition of the need to combine such separate perspectives and layers can already have \textit{by itself} positive effects for the effective protection of individuals. In particular, an open discussion of the values that the different provisions of the e-Privacy Directive aim to serve will help to reduce ambiguities in the analysis of the legal challenges to be addressed.

The complementarity of the three approaches needs to be emphasised. One can find an example of this complementarity in their capacity to cope with different challenges triggered by the large-scale reliance on data mining and profiling practices. From the standpoint of personal data protection, profiles deserve special attention inasmuch as they involve the processing of personal data and as they are sets of data related to identified or identifiable individuals. From the perspective of the right to privacy, there is a need to address the not-less-important issue of the \textit{impact} of profiling on individuals. From the point of view of technology-focused protection, there is a need to deal with the issue of the generation, collection, dissemination and processing of seemingly non-personal data to be mined for the construction and attribution of profiles.

\textbf{8.5.1 Upgrading personal data protection}

A first group of legal responses to the challenges of the ubiquitous Information Society deals with the refinement and updating of key definitions and key provisions of the current legal development of the right to the protection of personal data as recognised by Article 8 of the

\textsuperscript{684} It might be worth recalling that this study focuses on privacy and trust and is not meant to cover directly the legal responses needed to cope with other ethical and legal concerns related to the ubiquitous information society, even if they might be intimately linked. This refers notably to human dignity, integrity or autonomy.


EU Charter of Fundamental Rights. The key EC legal instrument in this regard is the Data Protection Directive, following the approach initiated by Council of Europe Convention 108. Complementarily, relevant provisions appear in the e-Privacy Directive.

**Reviewing definitions of key data protection concepts**

Reviewing key definitions used in EC data protection provisions is necessary to make sure that the legislation is fully adapted to new practices and realities. This concerns in particular the concepts of “personal data” and of “data processor” and “data controller”.

Clarification of the concept of personal data appears to be necessary in the light of its persistent divergent interpretations, especially in the context of new practices. The basic requirements for such elucidation should be that the definition is operative and that it effectively protects individuals. The Article 29 Working Party contribution to the clarification has certainly provided a useful reference for discussion, but no consensus appears to have been reached among the industry and practitioners on the interpretation of the concept. Some have suggested that a definition of personal data based on the identifiable nature of the subject might not be operative, and that other criteria could be used, e.g., biographical data, identifiers linked to persons or terminal equipment and/or points of contact. It has also been pointed out that any re-definition of the notion should consider the possible need to refocus protection away from the “personal” dimension of the data. The clarification of the concept of personal data can also be left to eventual judicial review.

Another set of definitions to be reassessed refers to those of the entities responsible for the application of the rules regarding the protection of personal data, namely the definitions of data processor and data controller. In this case, the need for a response is triggered mainly by new developments challenging the current criteria for the distinction between the two roles.

**Establishing requirements for consent**

Consent plays a pivotal role in the implementation of data protection rules, but its collection and expression is being challenged by different current and expected developments. There is a consensus on the importance of strengthening it. In this context, a legal response should establish certain minimum requirements regarding the obtention and proof of consent, as well

---

687 ETS No. 108.
691 European Data Protection Supervisor, Comments of 2 September 2007 on selected issues that arise from the IMCO reports on the review of Directive 2002/22/EC (Universal Service) and Directive 2002/58/EC (ePrivacy), Brussels, p. 3.
as withdrawal of consent. Recent legal developments at national level have taken place in this direction.\textsuperscript{692}

To better regulate consent, it has been suggested that the EC should consider adopting more detailed standards on when consent can be given,\textsuperscript{693} as well as the limits to the validity of consent.\textsuperscript{694} The regulation of consent in the processing of sensitive data might require special attention, for instance, through specific provision on the use of cookies and similar active elements in the context of e-health services.\textsuperscript{695} Certain special requirements could be established for the consent of minors. Requiring consent to the disclosure of certain categories of data (such as location data) by minors could be considered illegal.\textsuperscript{696}

**Detailing requirements for the lawfulness of processing**

Consent can only be genuine in the context of real, informed choice. Informed consent is therefore structurally linked to transparency of data collection and processing. More concrete obligations on the fairness of transparency requirements for processing might be required. Important issues to be considered include the information to be given to the data subject, the data subject’s right of access and the data subject’s right to object (and, in particular, the scope of this latter right).

**Guaranteeing lawfulness of processing in profiling practices**

Various provisions of the Data Protection Directive might require more detailed determination regarding profiling practices and, in particular, the access to the knowledge generated by such practices.\textsuperscript{697} Special consideration should be given to techniques and practices that modify the nature of the data processed (e.g., that turn data not falling under “special categories of data”\textsuperscript{698} into data falling under such categories)\textsuperscript{699}, the information to be given to the data subject on the processing and the data subject’s right to object to it. Concretely, the provision on automated individual decisions\textsuperscript{700} should specify under which conditions it can be considered that measures laid down by the laws authorising automated individual decisions effectively safeguard the data subject’s legitimate interests.

---


\textsuperscript{693} Hogan & Hartson and Analysys, *Preparing the Next Steps in Regulation of Electronic Communications - A contribution to the review of the electronic communications regulatory framework*, Final Report, Study for the European Commission, July 2006, p. 15.


\textsuperscript{697} Hildebrandt, Mireille, and Serge Gutwirth (eds.), *Profiling the European Citizen: Cross disciplinary perspectives*, Springer Science, Dordrecht, 2008; see especially p. 283.

\textsuperscript{698} Article 8 of Directive 95/46/EC.


\textsuperscript{700} Article 15 of the Data Protection Directive.
Simplifying the determination of applicable law

The limitations of the current provisions on applicable law call for new approaches. The general practice of collecting personal data as a condition for access to certain services, combined with the recognition of the data subject as the weakest part in its relation with data controllers and processors, encourages the adoption of consumer law approaches. Member States could adopt a rule that data processors providing services directed towards the EU be governed by the law of the country where the user is habitually resident.

Clarifying obligations for the disclosure of personal data

If national developments create distortions or obstacles in the functioning of the internal market, the “Promusicae” judgement justifies an EC determination of the circumstances for the disclosure of personal data by certain data controllers such as Internet service providers. Such a determination would have to follow the European Court of Justice acknowledgement of the need to carefully balance the protection of privacy and personal data with other relevant rights.

Empowering data protection authorities

Enforcement of data protection legislation is directly linked to the monitoring tasks of national and sub-national Data Protection Authorities (DPAs). Although their joint work in the context of the Article 29 Working Party certainly favours common interpretations of dispositions and homogeneous approaches, a legal response to persistent discrepancies in their activities needs to be carefully considered. A legal response might be necessary if the discrepancies create distortions or obstacles to the functioning of the internal market. There are discrepancies in their independence, their powers and duties (DPAs have different levels of investigatory powers) and in the sanctions and penalties they can impose. The current proposal for amending Directive 2002/58/EC would strengthen their investigation powers and resources and allow cessation of infringements.

Effectively encouraging enforcement

Enforcement is one of the main challenges for data protection in the ubiquitous Information Society. One can envisage responses to encourage it. Judicial intervention could help. New provisions could allow legal persons to ask for damages for infringements of the e-Privacy Directive, for instance, regarding spam. Class actions could also be considered. Similar measures could help enforce compliance with the Data Protection Directive.

8.5.2 Developing privacy protection

The protection of the right to privacy in the ubiquitous Information Society cannot rely

---

704 European Data Protection Supervisor, Opinion of 10 April 2008, op. cit.
705 Ibid.
exclusively on the development and implementation of the right to protection of personal data. Some might view the legal development of the fundamental right to privacy as stated in Article 8 of the European Convention of Human Rights and Article 7 of the EU Charter of Fundamental Rights as rather limited, especially compared to EC the legal development of the right to the protection of personal data. An effective legal reaction to the identified challenges should bring more substance to this right at EC level.

The second group of legal responses to the privacy and trust challenges of the ubiquitous Information Society focuses on the development of such a right, from different perspectives.

**Privacy of communications**

Revising the provision\(^{706}\) in the e-Privacy Directive regarding confidentiality of communications might ensure better compliance with Article 7 of the Charter. The scope of the provision should be wider to cover better the types and means of communications and the confidentiality of personal data. Differing national approaches to the monitoring and filtering of communications\(^{707}\) as well as the processing of IP addresses for advertisement purposes suggest a need for better harmonisation.\(^{708}\)

Some have suggested recognition of a right to anonymity and that individuals should have the right to remain non-identifiable when sending messages, at least not identifiable by certain parties.\(^{709}\) Legal responses to ensure effective respect of the right to privacy of communications should take into account its formal nature in different national constitutional traditions, and the fact that a right to anonymity of communications cannot in principle be considered a fully equivalent right, especially when anonymity is considered only a *relative* value.\(^{710}\)

**Including privacy of stored communications**

Guaranteeing the confidentiality of communications requires protection not only of their transmission, but also of their storage. The relevance of this issue at EC level is certainly acknowledged in Directive 2002/58/EC, which includes a provision imposing on Member States the obligation to ensure certain requirements for the use of electronic communications

---

\(^{706}\) Article 5 of Directive 2002/58/EC.

\(^{707}\) Be it for the enforcement of IPRs, the protection of children or to serve any other interest. For recent Italian jurisprudential developments on the surreptitious collection by private companies of IP addresses to be used against alleged fraudulent uses of material protected by copyright, see: Mari, Gaia, “Saggi - L'Unione Europea impone di non sacrificare ad occhi chiusi la proprietà intellettuale sull'altezza della privacy”, *Il diritto di autore*, No. 3, 2008, pp. 289-321. Regarding the need to take into account data protection concerns while developing strategies to protect children online, see European Data Protection Supervisor, Opinion of the European Data Protection Supervisor on the Proposal for a Decision of the European Parliament and of the Council establishing a multiannual Community programme on protecting children using the Internet and other communication technologies, Brussels, 23 June 2008.

\(^{708}\) Poullet and Dinant, op. cit., p. 51.

\(^{709}\) In the view of the IWG, international law should unequivocally establish that the process of communicating (including communications via electronic mail) is protected by the secrecy of telecommunications and correspondence. See International Working Group (IWG) on Data Protection in Telecommunications, *Working Paper on Telecommunications Surveillance, 31st Meeting*, Auckland, 26-27 March 2002.

networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user. New developments as described in the previous sections call for a more solid protection of terminal equipment.

Such protection should respond to the different national approaches regarding privacy of communications as described in the preceding paragraphs. It could also strongly benefit from the understanding of terminal equipment in terms of “digital territory” (see section 4.4), which would draw attention to need to protect certain types of terminal equipment with the same guarantees as the home is protected by the EU Charter and national legal frameworks. Recent national developments such as the recognition of a right to the confidentiality or integrity of technological information systems (described in Chapter 6) could be one of the possible legal responses in this direction. It this context, some have proposed a similar “users’ right to full control of terminal equipment”.  

The right of the citizen-consumer to be left alone

The right to privacy implies that individuals should be free of interference in their private lives. It is not only about protecting communications or privacy of the home, but also about respect for private life. One can trace this understanding of the right to privacy through a series of EC legal developments, even if they do not explicitly refer to it: for instance, the provisions concerning advertising practices in the “Television without Frontiers” Directives of 1989 and 1997 and in the 2007 Audiovisual Media Services Directive. Regulation of unsolicited communications follows the same logic as explained in Recital 40 of the e-Privacy Directive, safeguards against unsolicited communications are provided to protect subscribers against undue intrusions of their privacy. The regulation of unsolicited communications is therefore not grounded on the processing of personal data; what is at stake is the privacy of individual, not the processing of data as such. This phenomenon of protecting privacy as respect for the enjoyment of private life has induced certain authors to identify an emerging right of the consumer to be left alone.

A legal response to the new interferences with privacy can be configured around the need to protect users and consumers against not only invasive advertising practices and unsolicited communications, but also unsolicited adjustments interfering with their privacy. While the

715 One of the key innovations introduced by Directive 2002/58/EC was the regulation of unsolicited communications (Article 13).
advent of the ubiquitous Information Society makes it increasingly difficult to determine what a communication is and which categories of communications are to be specially protected, profiling practices proliferate and new marketing strategies develop. In this context, devices and applications can be programmed not only to display or convey certain sets of information, but also to adapt their performance in specific circumstances. Rules to counter the negative effects of the development of such adjustments might establish an opt-in regime guaranteeing that the individual is able to consent to or refuse such practices.

8.5.3 Embracing the technological dimension

Technologically neutral approaches for the protection of personal data and privacy can be complemented by other approaches that anchor protection in the technology itself. Certain elements of Directive 2002/58/EC can be interpreted as steps in this direction.717

Special protection for certain categories of data

A response following this logic would consolidate the incipient approach in Directive 2002/58/EC by unambiguously clarifying that certain categories of data deserve and require special protection regardless of their legal qualification as personal or non-personal data.

The utility of this approach can be illustrated with a reference to IP addresses. The discussions about whether IP addresses should be considered as personal data and in which circumstances have not yet considered with enough detail the possibility of regarding IP addresses as data whose processing should be submitted to conditions and limitations regardless of their personal nature, or of their qualification as traffic data in the sense of Directive 2002/58/EC.718 This approach would tend to ensure that they are protected in all suitable circumstances. In its Opinion of 4 April 2008 on search engines, the Article 29 Working Party examined the processing of IP addresses by search engines and recommended a maximum storage period of six months. This could serve as a starting point to discuss general regulation of processing of this and equivalent types of data, including processing of communications-related data not currently covered by the e-Privacy Directive.

There might also be a need to regulate location-related data even if such data do not relate to users or subscribers of public communications networks or publicly available electronic communications services.719 The Article 29 Working Party has provided guidance on consent and information requirements for location data,720 and has considered in more detail location of minors and employees. In locating employees, the Working Group considers the collection excessive in situations where employees would be free to make their own travel arrangements or where the location monitoring is done for the sole purpose of monitoring employees and other means are available. Location information should not be collected outside of working hours, and the Working Group recommends that location equipment which is also used for private purposes permit employees to turn off location tracking. This could serve as a basis

718 See, for instance: European Data Protection Supervisor, Comments of 2 September 2008 on selected issues that arise from the IMCO reports on the review of Directive 2002/22/EC (Universal Service) and Directive 2002/58/EC (ePrivacy), Brussels.
719 As currently required to trigger applicability of Article 9 of Directive 2002/5/EC.
for discussion of more general provisions for location-related data.

Is there a need to regulate other categories of data, especially in the light of deployment of RFID and the emergence of the Internet of things? Facilitating information exchanges for RFID-equipped items might require a specification of (a) the information on the chips (unique identification numbers), (b) the retrieval of information from applications using unique identification numbers, and (c) the aggregation and interpretation of related data such as location-related data.\footnote{221} There may be a need for new regulation covering the use of unique identification numbers, or of any other data allowing for the identification of objects or devices.

The automatic inclusion of any such data in digital files needs examination. Users should be able to produce digital content (texts, images, audio, etc.) free from any persistent identifiers, not only to protect their privacy, but also to ensure freedom of expression, especially as digital user-generated content is increasingly shared and distributed.

**Requirements for terminal equipment**

Terminal equipment may need to comply with certain specific requirements minimising emission, storage and processing of communication-related, location-related or other relevant data.\footnote{222} Such requirements might be useful for specific technologies, such as RFID, and to address issues such as network chatter.\footnote{223} The Article 29 Working Party has already expressed its support for legal provisions on the deployment by data controllers of privacy-enhancing technologies (PETs) applying the principle of data minimisation.\footnote{224}

## 9 EU LEVEL INSTRUMENTS TO ENACT OR SUPPORT THE IDENTIFIED MEASURES

The European Commission has a set of instruments at its disposal which it can use to support and trigger the implementation of responses. Instruments include social dialogue, fostering technical development, international co-operation, ensuring a regulatory framework enabling citizens, businesses and public entities to achieve the maximum of the potential benefits, its grant programmes, policy initiatives and different ways to support co-operation of Member States and of stakeholders. In this chapter, we give some examples of the instruments which can be used to implement most of the responses referenced in the preceding chapter. The following table summarises which instruments can be used to implement which responses. In some cases, a response can be implemented by means of more than one instrument.

<table>
<thead>
<tr>
<th>Instruments</th>
<th>Responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Research</td>
<td>• Technical responses</td>
</tr>
<tr>
<td></td>
<td>• Benchmarking, metrics and additional research</td>
</tr>
<tr>
<td></td>
<td>• Audits and more resources for DPAs</td>
</tr>
<tr>
<td></td>
<td>• Testing third-country data protection safeguards</td>
</tr>
<tr>
<td></td>
<td>• Evaluation of privacy aspects of ICT research proposals</td>
</tr>
<tr>
<td>Demonstration projects</td>
<td>• Technical responses</td>
</tr>
<tr>
<td></td>
<td>• Privacy and trust seals</td>
</tr>
<tr>
<td>Social dialogue, impact</td>
<td>• Open working groups</td>
</tr>
<tr>
<td>assessments and consultations</td>
<td>• Sharing best practices</td>
</tr>
<tr>
<td></td>
<td>• Public education and awareness-raising</td>
</tr>
<tr>
<td></td>
<td>• Media attention, publicity and public opinion</td>
</tr>
<tr>
<td></td>
<td>• Transparency and trust-enhancing responses</td>
</tr>
<tr>
<td>Ensuring an appropriate</td>
<td>• Privacy and trust seals</td>
</tr>
<tr>
<td>regulatory framework</td>
<td>• Open working groups</td>
</tr>
<tr>
<td></td>
<td>• Standards</td>
</tr>
<tr>
<td></td>
<td>• Codes of conduct</td>
</tr>
<tr>
<td></td>
<td>• Transparency and trust-enhancing responses</td>
</tr>
<tr>
<td>International co-operation</td>
<td>• Privacy and trust seals</td>
</tr>
<tr>
<td></td>
<td>• Open working groups</td>
</tr>
<tr>
<td></td>
<td>• Standards</td>
</tr>
<tr>
<td></td>
<td>• Codes of conduct</td>
</tr>
<tr>
<td></td>
<td>• Transparency and trust-enhancing responses</td>
</tr>
<tr>
<td>Procurement</td>
<td>• Procurement</td>
</tr>
<tr>
<td></td>
<td>• Technical responses</td>
</tr>
</tbody>
</table>

Of the responses identified in Chapter 8, only three have not been captured in the above table, namely Industry initiatives (section 8.4.3), Training staff (8.4.4) and Individual initiatives.
(8.4.5), which is understandable since the instruments under discussion here are those at the disposition of the Commission.

9.1 RESEARCH

The Commission’s ability to conduct and/or fund research is a powerful instrument by means of which it can develop responses to privacy challenges. The research can take different forms or be carried out in different ways. Surveys and the gathering of statistical data, such as that undertaken by Eurobarometer, is one example. Reference has already been earlier in this study to the recent Eurobarometer February 2008 report on Data Protection in the European Union: Citizens’ perceptions.

The research undertaken by DG Research’s Joint Research Centre is another. The Framework Programmes under which the Commission funds or gives grants to trans-European partnerships to undertake research on issues and technologies that offer promising possibilities for Europe or that vex policy-makers. Many of the projects supported under FP5 and FP6 have explored and/or developed privacy-enhancing technologies (PETs). GUIDE, PAMPAS, PISA, PRIME, RAPID and STORK are examples. The Commission can also issue tenders for research (such as that under which this study is being performed).

Some of the other instruments mentioned in this chapter, such as demonstration projects, impact assessments and consultations, can also be regarded as forms of research, but we have put them under separate sub-headings, because they are rather more specific instruments that are used or can be used in specific contexts.

9.2 DEMONSTRATION PROJECTS

The Commission has financially supported various demonstration projects undertaken by other stakeholders, notably industry, sometimes in conjunction with Member States. Section 3.2.4 refers to one such project, the Smart Open Services (SOS) project, which among other things, will test and demonstrate the cross-border interoperability of electronic health record (EHR) systems. As previously mentioned, the SOS project is co-funded by the European Commission and supported by 12 Member States and their industry players.

Section 4.3.3 on the state of play regarding biometric passports and identity cards refers to another such project called STORK (Secure idenTity acrOss boRders linKed). The project will build on existing systems and try to find common e-ID specifications that can be further developed and gain wider agreement. The EC and participating partners are funding the project to the tune of €20 million.

Projects are a useful instrument for at least two main reasons. One is to test the feasibility of, for example, new privacy-enhancing technologies. Another is to demonstrate the feasibility to other stakeholders, including the public, and thereby build support for an operational system or service, such as electronic health records. The Commission and/or other stakeholders might wish to build support, not only in the form of public opinion, but also in the form of standards.
9.3 SOCIAL DIALOGUE, IMPACT ASSESSMENTS AND CONSULTATIONS

As an instrument, “social dialogue” initiated by the EC can take different forms. The EC can issue press releases, can encourage citizens to use its websites such as “Your Voice in Europe,” convene workshops and conferences or speak at those organised by others, can have Commissioners and their staff speak on the various issues of the day. Eurobarometer can survey European opinion. The Commission can initiate public consultations. For example, as noted above in section 3.2.4, there seems to be need for a wide-ranging debate and consultation on electronic health records and, in particular, the privacy impacts.

To stimulate the debate on social networking and children, the Commission organised a Safer Internet Forum in Luxembourg in September 2008. About 300 participants from NGOs, industry, and public authorities attended. The Commission launched a public consultation on social networking and child safety and published the results online. As a further measure, it convened a social networking task force, which met with operators of social networking sites, researchers and child welfare organisations. As Information Society Commissioner Viviane Reding favours self-regulation, the task force is expected to agree guidelines to be adopted voluntarily by the European industry.

Consultations, like that employed by the Commission with regard to RFID, are useful instruments in developing appropriate responses to the prospective deployment of new technologies and applications where there is uncertainty about what responses are indeed appropriate. Waldo et al. have highlighted many uncertainties with regard to e-health, as mentioned in section 3.2.4, and have argued in favour of a wide-ranging public debate on the issues raised by electronic health records. Consultations have many benefits, for example, in identifying pros and cons, in gathering information that policy-makers might not have considered adequately, in moving toward consensus among stakeholders, in testing policy options, as a public relations exercise (in the best sense of that term) in giving stakeholders, including the public, an opportunity to air their views, as an exercise in democracy, and so on. To be effective, consultations should be conducted before policy-makers have decided what they intend to do (i.e., they should not be mere public relations exercises, in the negative sense of that term). Consultations can take many different forms (open meetings, stakeholder workshops, consensus conferences, Delphi exercises, online questionnaires, surveys, etc.) and one or more of those forms may be appropriate depending on the issue, context, the objectives of the policy-maker, public concerns and so on.

Consultations can be held as stand-alone or exercises or as part of a (privacy) impact assessment.

In analysing new technologies that are likely to raise significant policy issues, one can carry out a privacy impact assessment (PIA). The Commission already conducts impact assessments (IA) in its development of significant policies and programmes. It is useful to distinguish, however, between impact assessments of the type the Commission already carries out and privacy impact assessments.

725 http://ec.europa.eu/yourvoice/
Impact assessments

The Commission promulgated a set of Impact Assessment Guidelines in 2002, as part of its Better Regulation package, which were subsequently revised in 2005 and 2008. The Commission defines impact assessment as “a process aimed at structuring and supporting the development of policies. It identifies and assesses the problem at stake and the objectives pursued. It identifies the main options for achieving the objective and analyses their likely impacts in the economic, environmental and social fields. It outlines advantages and disadvantages of each option and examines possible synergies and trade-offs.”

Impact assessment is an aid to political decision, not a substitute for it. It gathers and presents evidence that helps in determining possible policy options and their comparative (dis)advantages. It informs decision-makers of the likely impacts of proposals, but it leaves it up to them to take the decisions.

In addition to impact assessments, and often a part of them, another important instrument in policy development is consultation, the gathering of opinions and information from interested parties. Consultation enhances the transparency of the policy-development process and ensures that proposed policy is practically workable and legitimate from the point of view of stakeholders. Furthermore, the Commission is required by the EC Treaty to carry out wide consultations before proposing legislation (see the Protocol on the application of the principles of subsidiarity and proportionality). The Commission set out its minimum standards for consultation in 2002 as part of the same its better regulation package.

Stakeholder consultation and collection of expertise can run throughout the impact assessment process.

An impact assessment essentially addresses these analytical questions:

- What is the problem or issue for which a policy appears necessary? What is the nature, magnitude and evolution of the problem? Why assess the problem? How should the problem be assessed? Does the Union have the right to act? How would the problem evolve if the current EU approach were to continue?
- What objectives should the Union pursue in the context of the problem? Are they consistent with other EU policies and strategies?
- What are the main policy options for reaching these objectives?
- What are the likely economic, social and environmental impacts of those options?
- What are the advantages and disadvantages of the main options? How do the options rank?
- How should the chosen option be monitored and evaluated? What evaluation criteria are to be used?

An IA need not involve a long and detailed study in every case, but it should allow for an informed debate in all cases.

In their existing form, the catalogue of “key questions” is largely dominated by economic and  

---

728 http://ec.europa.eu/governance/better_regulation/impact_en.htm
ecological considerations. Social impact issues – which are arguably more difficult to measure and assess – play only a minor role. In fact, privacy is mentioned only once in the IA guidelines: "Does the option affect the privacy of individuals (including their home and communications) or their right to move freely within the EU?" Trust is not a key issue in the European impact assessment guidelines at all. Since the Impact Assessment Guidelines are constantly improved and updated, it would be an option to include privacy and trust more visibly.

Privacy impact assessments

A privacy impact assessment (PIA) more specifically addresses the privacy impacts of a new technology, policy, programme or project, rather than all impacts. A few countries, such as the UK, the US, Canada, Australia and New Zealand, use PIAs. The US Department of Homeland Security defines a PIA as “an analysis of how personally identifiable information is collected, used, disseminated and maintained”. The UK Information Commissioner’s Office (ICO) defines a PIA as “a process whereby the potential privacy impacts and implications of a project are identified and examined from the perspectives of all stakeholders, and an attempt is made to find ways to minimise or avoid harms”. The italics have been added to highlight the implication that a PIA is a tool for involving all stakeholders in the assessment process.

Roger Clarke, one of the earliest proponents of privacy impact assessments, identifies the key characteristics of a PIA, as follows:

- **a PIA is performed on a project or initiative** (i.e., a PIA is distinct from an organisational privacy strategy);
- **a PIA is anticipatory in nature**, conducted in advance of or in parallel with the development of an initiative, rather than retrospectively (i.e., a PIA is distinct from a privacy audit);
- **a PIA has broad scope in relation to the dimensions of privacy**, enabling consideration of privacy of the person, privacy of personal behaviour and privacy of personal communications, as well as privacy of personal data (i.e., a PIA is distinct from a mere ‘data privacy impact assessment’);
- **a PIA has broad scope in relation to the perspectives reflected in the process**, taking into account the interests not only of the sponsoring organisation, and of the sponsor's strategic partners, but also of the population segments affected by it, at least through representatives and advocates (i.e., a PIA is distinct from an internal cost/benefit analysis or internal risk assessment);
- **a PIA has broad scope in relation to the expectations against which privacy impacts are compared**, including people’s aspirations and needs, and public policy considerations, as well as legal requirements (i.e., a PIA is distinct from a compliance assessment, whether against privacy laws generally, or data privacy laws in particular, or a specific data protection statute);
- **a PIA is oriented towards the surfacing both of problems and of solutions to them** (i.e., a PIA is more than just a privacy issues analysis);
- **a PIA emphasises the assessment process** including information exchange, organisational learning, and design adaptation (i.e., a PIA is not merely focussed on the expression of a carefully-worded privacy impact statement);
• a PIA requires intellectual engagement from executives and senior managers (i.e., a PIA is not a mere checklist ticked through by junior staff or lawyers).\textsuperscript{730}

Recently, the ISO has produced a standard for PIAs in financial services.\textsuperscript{731} In 28 pages, ISO 22307:2008 describes the privacy impact assessment activity in general, defines the “common and required components” of a privacy impact assessment, and provides guidance. ISO distinguishes a privacy compliance audit from a privacy impact assessment in that the compliance audit determines an organisation’s current level of compliance with the law and identifies steps to avoid non-compliance, whereas a PIA is used to identify ways to safeguard privacy.

The most detailed set of privacy impact assessment guidelines are those developed in the UK Information Commissioner’s Office (ICO).\textsuperscript{732} The European Commission specifically refers to the ICO guidelines in its draft RFID Recommendation.\textsuperscript{733} In Article 3 of its draft RFID Recommendation, the Commission says that before an RFID application is implemented, the RFID application operators should conduct, individually or jointly within a common value chain, a privacy impact assessment to determine what implications its implementation could raise for privacy and the protection of personal data, and whether the application could be used to monitor an individual. The level of detail of the assessment should be proportionate to the risks associated with the particular RFID application. The assessment should comply with good practice frameworks to be established in a transparent way in partnership with all relevant stakeholders, and in consultation of the relevant supervisory data protection authorities.

The UK PIA distinguishes between “small scale” and “full scale” privacy impact assessments. The ICO says it is not feasible to write a “one size fits all” guide, so for each project, some parts of its PIA handbook will not be relevant. The scale of effort that is appropriate to invest in a PIA depends on the circumstances. A project with large inherent risks warrants much more investment than one with a limited privacy impact. Other projects may merely need a check of their compliance with privacy laws.

The ICO says a PIA should be conducted at an early stage of a project. A PIA examines broad questions about privacy impacts and individuals’ perceptions.

Privacy has to be balanced against many other, often competing, interests. The practical approach to privacy protection is therefore to find appropriate balances between privacy and those multiple competing interests.

Among the questions typically addressed by a PIA are the following:
• What information is to be collected, from whom, why and how?
• What is the legal basis for doing so?

\textsuperscript{733} Draft Recommendation on the implementation of privacy, data protection and information security principles in applications supported by Radio Frequency Identification (RFID). http://ec.europa.eu/yourvoice/ipm/forms/dispatch/?form=RFIDRec
• What are the privacy risks and how can they be mitigated?
• Have stakeholders been consulted about the project, its alternatives, impacts and risks?
• How are data to be used (and reused)? Will data subjects be informed about any repurposing? Can they object?
• What types of tools are used to analyse the data and what type of data may be produced?
• How will data be secured? Who will have access to the data?
• How will the information be checked for accuracy?
• Will data subjects be given chance to confirm accuracy and correct errors?
• How long will data be retained?
• Will data be shared with others? Why? Under what conditions?
• Do individuals have an opportunity and/or right to decline to provide data?
• What are procedures for allowing individuals to gain access to their data?
• Are there less privacy-intrusive alternatives?
• What accountability exists?
• What recourse do data subjects have re abuse or misuse?
• What auditing measures and technical safeguards will be put in place?
• What design choices were made to enhance privacy?
• Does the project involve new linkages of personal data with data in other collections?
• Does the project involve new or changed data collection policies or practices that may be unclear or intrusive?
• Does the project involve new or privacy-invasive technologies?
• Will data be transmitted outside the EU? What safeguards exist?

A PIA usually results in a PIA report, which may be published or distributed to stakeholders. One could expect to find these elements in a PIA report:
• A description of the project
• An analysis of the privacy issues arising from it
• The business case justifying privacy intrusion and its implications
• Discussion of alternatives considered and the rationale for the decisions made
• A description of the privacy design features adopted to reduce or avoid privacy intrusion and the implications of these design features
• An analysis of the public acceptability of the scheme and its applications.

Differences and similarities between impact assessments and privacy impact assessments

IAs and PIAs bear some similarities and differences. Both may involve consultations with stakeholders. Both could be regarded as a form of risk assessment. In the EC context, however, an impact assessment has a broader remit in assessing the social, economic and environmental impacts of policies and programmes and the different policy options. A PIA is more appropriate in assessing the privacy impacts of a specific project, service, system or policy and how they can be minimised. An impact assessment could be regarded as appropriate at a rather higher policy level, whereas a privacy impact assessment could be regarded as more appropriate at a project or service level, but perhaps one should not be too dogmatic on that point. In Canada, for example, federal policy requires all government institutions, except the Bank of Canada, to conduct and document PIAs for proposals for all new programmes and services that raise privacy issues. “The assessment process is not

734 Treasury Board of Canada Secretariat, Privacy Impact Assessment Policy, pp.1-4.
intended for the development of new legislation. It is intended to be adapted to suit particular institutional program and service requirements.” In the United States, the Electronic Government Act of 2002 requires that federal agencies “conduct a privacy impact assessment, ensure the review of that assessment by the Chief Information Officer or equivalent official, and make such assessment publicly available, before: (1) developing or procuring IT that collects, maintains, or disseminates information that is in an identifiable form; or (2) initiating a new collection of information that will be collected, maintained, or disseminated using IT and that includes any information in an identifiable form.”  

The key criterion about whether a PIA should be conducted is: does the new project, policy, programme, system, technology or whatever involve personal data and is it likely to have privacy impacts?

9.4 ENSURING AN APPROPRIATE REGULATORY FRAMEWORK

The insurance of an appropriate regulatory framework has been a constant feature of the different EC policy frameworks for the information society. The current policy framework, the i2010 initiative, foresees as an element of paramount importance for the effective creation of a Single European Information Space the provision of a regulatory framework providing proper security and protection of privacy and personal data. In the context of this objective has been launched the ongoing review of the ‘electronic communications package’, which includes a series of amendments for Directive 2002/58/EC. Guaranteeing an appropriate regulatory framework will certainly be also of capital importance in the post-i2010 policy framework for the information society, in which the realisation of a trustworthy ubiquitous information society might be a top priority.

In principle, in order to ensure that the regulatory framework is able to cope with the challenges of the ubiquitous information society, there are basically three possible strategies: (1) to maintain the established regulatory framework unaltered but accompany it with new interpretative or implementation guidance; (2) to adapt the regulatory framework by reforming it; and (3) to introduce new solutions, possibly even outside of the scope of the current framework.

Formally, the measures available at EC level for the insurance of an appropriate regulatory framework range from the introduction of new legislative initiatives to the use of ‘soft law’ techniques. ‘Soft law’ approaches are best suited to ensure appropriateness of the regulatory framework without actually modifying it.

The regulatory framework can support the implementation of not only what has been described as ‘legal responses’, but also of other types of responses. This is for instance the case of co-regulation through codes of conduct. This section considers types of measures that could be used to design an appropriate regulatory framework for privacy and trust in the post-i2010 policy framework.

735 http://thomas.loc.gov/cgi-bin/bdquery/z?d107:HR02458:@@@L&summ2=m&
Option 1: No new legislative proposal

The appropriateness of the regulatory framework could in principle be sought after without the introduction of any legislative proposal to amend it or complement it. If its provisions are considered sufficient and fundamentally appropriate, other measures can be put in place contributing to its (better) implementation. ‘Soft law’ techniques can notably contribute to complement and refine the legislative framework. The EC Communication on the follow-up of the Work Programme for better implementation of the Data Protection Directive notably concluded that there was no need to for the EC to submit legislative proposals to amend Directive 95/46/EC.736 Nevertheless, it identified areas in which further action was required.

In this sense, the EC has chosen to support the deployment of PETs through an ad-hoc Communication.737 The Communication considered the benefits of PETs and set out an approach to support their development and their use by data controllers and consumers. In a similar approach, the EC is expected to publish imminent a Recommendation on the application of general data protection rules for the use of RFID systems.738 It has also announced the publication of a Communication on Privacy and Trust in the ubiquitous information society (currently under preparation).739 The opinions of the Article 29 Working Party can be also crucial in providing guidance on the regulatory framework, and the EC can request specific guidance on specific issues.

There is still another tool at the disposal of the EC to implement some of the identified responses without actually changing the regulatory framework, but making use of certain provisions that it contains and that have remained until now unused. Article 14 (3) of Directive 2002/58/EC establishes that measures may be adopted to ensure that terminal equipment is constructed in a way that is compatible with the right of users to protect and control the use of their personal data, in accordance with Directive 99/5/EC.740 This Directive provides in its Article 3.3(c) that the Commission may decide, through a comitology procedure, that apparatus within certain equipment classes or apparatus of particular types shall be so constructed that they incorporate safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected. In order to make the use of the concept of 'privacy by design' compulsory, the EDPS has recommended that the Commission makes use of this mechanism, in consultation with the RFID Expert Group.741

Option 2: Legislative reform proposals

Fully implementing certain responses identified as suitable might require nevertheless introducing modifications to the regulatory framework. The main relevant legal texts already foresee a systematic review of their provisions, in order to identify the eventual need for updating.

A basic criterion for the selection of the most suitable legal tool to implement the responses identified shall be to carefully assess they rationale. As described in the ‘legal responses’ section, a series of the suggested legal responses refer to an upgrading of the legal development of the right to data protection. This development, however, must take place avoiding any unnecessary fragmentation of EC data protection obligations.742

Similarly, future review of the legal framework might be used to clarify, on the one hand, the extent to which Directive 2002/58/EC (or any future Directive replacing it) particularises Directive 95/46/EC, and, on the other hand, the extent to which it does not particularise but complement it. This shall be strongly beneficial to ensure uniform understanding, and therefore implementation, of any of its provisions.

Even if the Data Protection Directive and the e-Privacy Directive can be considered the central elements of the regulatory framework for privacy in the ubiquitous information society, provisions of other pieces of EC legislation might require also special attention. Thus, it is strongly recommended that the protection of privacy and personal data are considered horizontally during the preparation of any eventual future review of the EC regulatory framework for electronic communications.

Legislative reform proposals could address issues derived from the challenges and responses identified, such as: clarifying the scope of application of the e-Privacy Directive, currently applying to “the processing of personal data in connection with the provisions of publicly available electronic communication services in public communication networks”; substantiating the right to privacy of communications; including in the e-Privacy Directive a provision similar to Article 27 of Directive 95/46/EC to encourage the use of codes of conduct; regulating unsolicited automatic adjustments that interfere with the private life of users or consumers.

Option 3: Other legislative proposals

Legislative proposals can also go beyond mere ‘routine’ up-dates, by introducing more substantial changes. The EC has acknowledged that introducing specific legislation for privacy and data protection for the Internet of Things or RFID cannot be excluded where self-regulation or interpretation prove insufficient.743


743 European Commission, Early Challenges Regarding the “Internet of Things”, Commission Staff Working Document Accompanying the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Communication on future networks and the internet, 29.09.2008, Brussels, p. 8; European Commission, Communication from the
The European Data Protection Supervisor has expressed that the adoption of a proposal for Community legislation regulating the main issues of RFID-usage in relevant sectors is to be recommended in case the proper implementation of the existing legal framework would fail. The EDPS envisages such a legislative measure as a *lex specialis* vis-à-vis the general data protection framework. The legislative measure could actually also be configured as a separate measure, substantiating directly Article 7 of the Charter and not Article 8.

### 9.5 COMMITTEES, WORKING GROUPS, PLATFORMS AND AGENCIES

The Commission can create or be instrumental in the creation of stakeholder committees, working groups, platforms and agencies in response to privacy and security challenges.

The Article 29 Data Protection Working Party, the European Data Protection Supervisor (EDPS) and the European Network and Information Security Agency (ENISA) have their own legal basis in Community instruments adopted by the European Parliament and the Council. However, not all committees and working groups need to be formally established as platforms or agencies. They can be of short duration. The FP7-supported ThinkTrust project has established two working groups, one dealing with security and trust, the other dealing with privacy and trust. These working groups have an expected lifetime of about 18 months, to end 2009. The working groups each comprise about 20 experts from across Europe who have agreed to commit their time free of charge in order to develop recommendations for the Commission (DG Information Society and Media). Such working groups have value not only for the Commission in gaining the distilled views of a wide range of experts from different backgrounds, disciplines and Member States, but also for the experts themselves who have an opportunity to “network” with their peers and to exchange views, ideas and information, which may be useful in their further (paid) research.

Committees, working groups, platforms and agencies could be regarded as a form of social dialogue and consultation, but they can also be distinguished from social dialogue in the sense that they have an on-going life, perhaps of only short duration (as in the case of the ThinkTrust project), and an organisational structure and tend to deal with a variety of different (though perhaps inter-related) issues, whereas social dialogue tends to be focused on a specific issue. The former has a structure and a set of objectives, whereas the latter is an activity.

### 9.6 INTERNATIONAL CO-OPERATION

The Commission can stimulate international co-operation on a bilateral and multilateral basis in order to deal with transborder flows of personal data. As the Privacy Commissioner of Canada, Jennifer Stoddart, noted recently, “Protecting privacy, enhancing security and building user confidence… cannot be done on a country-by-country basis, the international

---


data flows are too great; the technologies are evolving too rapidly; and the jurisdictional challenges too daunting. The only way to achieve meaningful progress in such a complex environment is to work collectively on privacy and security issues. Internet privacy challenges have emerged on an international scale, and so require global thinking and global solutions.  

Ms Stoddart made some other good points too. She said, “We should be striving to achieve a basic level of privacy protection around the world. This does not mean we need to have a single, global standard, or one approach to protecting privacy, a misconception that can often make discussions between countries about how to best address privacy issues very challenging. Rather, countries should be encouraged to take different approaches to protecting privacy. Each local information environment is socially, culturally, economically and technologically unique. Policy-makers must abandon their comparative, legalistic approach, just as industry leaders must put aside their competitive, technological prejudices. Parochialism can be a significant barrier to the protection of privacy. Results matter more than local and national laws and achieving these results requires honest, global dialogue.”

One of the most important issues where global co-operation is needed is in regard to identity theft. The OECD has said, “ID theft could be made a specific offence, which is currently true in only a handful of countries. Sanctions could be increased to become more dissuasive across jurisdictions, which would discourage fraudsters from forum shopping (i.e. from evading regulatory compliance by locating in one country where sanctions would be low or inexistent and targeting consumers in another).” The rise in cybercrime has stimulated or renewed interest in international co-operation.

In addition to combating identity theft, there are many other privacy-related issues where international co-operation is unavoidable. Some issues can be dealt with on a bilateral basis. In other instances, multilateral co-operation, under the aegis of fora such as the OECD, ISO and ITU, is more appropriate. Of course, these multilateral fora also believe multilateral co-operation is necessary. For example, in its report on Malware: A Security Threat to the Internet Economy, the OECD calls on governments, the private sector, the technical and the civil communities to form a global “Anti-Malware Partnership” to find ways to reduce software vulnerabilities, raise awareness, establish codes of practice, and improve the coordination of CSIRTs.

Stimulating international co-operation, on either a bilateral or multilateral basis, is thus an important instrument at the disposition of the Commission in view of the fact that data flows so easily from one country to another.


746 OECD, “Governments give consumers a boost at high-level OECD meeting on the future of the Internet”, 18 June 2008. http://www.oecd.org/document/19/0,3343,en_2649_34267_40862227_1_1_1_1,00.html

9.7 PROCUREMENT

In section 8.2.4 above, we identified procurement as a response, but it can also be regarded as an instrument. The Commission’s ability to procure products and services means that it can, in effect, impose its own standards to ensure that those products and services are privacy-enhancing or, at least, privacy-protecting. It can also make specific procurements as a specific response to a specific challenge to privacy and trust. For example, it could ensure that all of its e-mail traffic is encrypted or that all of the computers, laptops, external hard drives and memory sticks that it procures can be switched on only with the biometric fingerprint of the Commission official to whom they are allocated.

We recognise that while procurement can be a powerful response to one or more challenges to privacy and trust, they are sometimes undertaken without maximising their instrumentality. For example, the EC might procure a batch of computers because it needs those computers, but not use the opportunity to impose a requirement for privacy-enhancing features.
10 ASSESSMENTS

This chapter has four sections. In the first, we identify criteria which can be used for assessing response measures, in particular, those discussed in Chapter 8. These are, in effect, ex ante criteria which can be applied by the Commission in deciding which responses are optimum for dealing with the challenges to privacy and trust such as those summarised in Chapter 7. The next section in this chapter identifies various indicators which can be used ex post for evaluating responses once they have been implemented. This section is relatively short and far from an exhaustive listing and assessment of indicators. It is meant only to provide examples of the types of indicators that can be used to assess measures once they have been implemented.

The third section of this chapter is more detailed and assesses the response measures discussed in Chapter 8 according to the criteria set out in section 10.1. In the fourth and last section of this chapter, we assess the responses in the context of the challenges in Chapter 7. Thus, in section 10.3 the responses are assessed as “free-standing” responses without reference to a specific challenge, whereas in section 10.4 we have clustered together the responses we think appropriate for each of the challenges and then assessed the effectiveness of the responses to a specific challenge.

10.1 CRITERIA FOR ASSESSING PROPOSED MEASURES

In its impact assessment on the Review of the EU Regulatory Framework for electronic communications networks and services, the Commission used the following factors to assess the impacts posed by each of three different options:748

- EU competitiveness
- Achievement of internal market
- Compliance cost for businesses
- Competition
- Innovation and investment
- Consumers
- Operators
- Administrative burden for national and European public administrations
- Employment and labour markets
- Social inclusion

We have reviewed these factors and have captured them as well as some others in the criteria we suggest below for assessing measures in response to the challenges to privacy and trust arising from new developments such as those described in Chapters 2 – 6 and summarised in Chapter 7 of this report. For each of the key criteria, we provide some questions which may be useful in clarifying what the criteria aim to assess.

---

<table>
<thead>
<tr>
<th>Impact</th>
<th>Key Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effectiveness</td>
<td>• Do the proposed measures address the problem and will they fix it, in whole or in part?</td>
</tr>
<tr>
<td></td>
<td>• Are there indicators to measure the effectiveness of the proposed measures, once they are implemented?</td>
</tr>
<tr>
<td></td>
<td>• Will the proposed measures contribute to ensuring stakeholder privacy and trust? If so, how?</td>
</tr>
<tr>
<td></td>
<td>• Are the proposed measures clear, understandable, not ambiguous?</td>
</tr>
<tr>
<td>Stakeholder support</td>
<td>• Are the proposed measures likely to be supported by or not likely to meet objections from stakeholders?</td>
</tr>
<tr>
<td></td>
<td>• Have stakeholders indicated their support (as a result of a consultation)?</td>
</tr>
<tr>
<td></td>
<td>• Do the proposed measures affect stakeholder participation in decision-making and, if so, how?</td>
</tr>
<tr>
<td>Time</td>
<td>• How long will it take to implement the measures? Is there a time factor at stake?</td>
</tr>
<tr>
<td>Opacity</td>
<td>• Do the measures prohibit unnecessary data collection and processing?</td>
</tr>
<tr>
<td></td>
<td>• Do the measures lead to minimising the amount of data to be collected?</td>
</tr>
<tr>
<td></td>
<td>• Do the measures avoid mission creep and limit the purpose of the response?</td>
</tr>
<tr>
<td></td>
<td>• Do the measures anonymise people, things and devices?</td>
</tr>
<tr>
<td>Transparency</td>
<td>• Do the measures enhance the participation of stakeholders?</td>
</tr>
<tr>
<td></td>
<td>• Do the measures provide user controls and respect for user rights?</td>
</tr>
<tr>
<td></td>
<td>• Do the measures provide for the availability of information about the collection, storage and/or processing of data?</td>
</tr>
<tr>
<td></td>
<td>• Do the proposed measures provide for oversight?</td>
</tr>
<tr>
<td></td>
<td>• Do the proposed measures include obligations for (self-)reporting by data controllers and/or processors/</td>
</tr>
<tr>
<td></td>
<td>• Do the proposed measures include provisions for auditing?</td>
</tr>
<tr>
<td>Enforcement</td>
<td>• Can the proposed measures be enforced (if there is a need for enforcement)?</td>
</tr>
<tr>
<td></td>
<td>• Do the proposed measures provide (technical) means for detecting or proving violations?</td>
</tr>
<tr>
<td>Economic effects</td>
<td>• Who will bear the cost of implementing the measures?</td>
</tr>
<tr>
<td>(resources and efforts)</td>
<td>• What are the costs involved?</td>
</tr>
<tr>
<td></td>
<td>• What resources or efforts are needed to implement the measures?</td>
</tr>
<tr>
<td></td>
<td>• Do the measures affect the functioning of the internal market and, if so, how? For example, do the measures have any effect on consumer choice or create barriers for suppliers or service providers?</td>
</tr>
<tr>
<td></td>
<td>• Do the proposed measures impact the competitiveness of EU companies?</td>
</tr>
<tr>
<td></td>
<td>• Do the proposed measures impact SMEs? For example, do they have to make investments to comply with the proposed measures?</td>
</tr>
<tr>
<td></td>
<td>• Do the proposed measures have cost implications for public authorities and, if so, how much are they expected to cost?</td>
</tr>
<tr>
<td>Impact</td>
<td>Key Questions</td>
</tr>
<tr>
<td>--------</td>
<td>--------------</td>
</tr>
<tr>
<td>Do the proposed measures affect or involve intellectual property rights?</td>
<td></td>
</tr>
<tr>
<td>Do the proposed measures stimulate or hinder innovation?</td>
<td></td>
</tr>
<tr>
<td>Do the proposed measures have consumer impacts? For example do they affect the costs consumers will have to pay for products or services? Do they affect the quality of products or services and, if so, how?</td>
<td></td>
</tr>
<tr>
<td>Do the proposed measures have any impacts on third countries? For example, is there a risk that the proposed measures might be seen as discriminating against third country suppliers or service providers?</td>
<td></td>
</tr>
<tr>
<td>Social impacts (other than privacy protection)</td>
<td>Do the proposed measures involve trade-offs against other social values, such as security? And, if so, what are the trade-offs?</td>
</tr>
<tr>
<td>Do the proposed measures affect employment and, if so, how? For example, will the proposed measures lead to an increase or decrease in employment?</td>
<td></td>
</tr>
<tr>
<td>Do the proposed measures have any impacts on job quality?</td>
<td></td>
</tr>
<tr>
<td>Do the proposed measures have any impacts on social inclusion? For example, do they help to bridge digital divides?</td>
<td></td>
</tr>
<tr>
<td>Do the proposed measures affect equal treatment or equal opportunity?</td>
<td></td>
</tr>
<tr>
<td>Do the proposed measures have any potential impacts on public health or safety?</td>
<td></td>
</tr>
<tr>
<td>Do the proposed measures lead to improvements in public awareness and education?</td>
<td></td>
</tr>
<tr>
<td>Do the proposed measures have any impacts on combating crime and/or terrorism?</td>
<td></td>
</tr>
<tr>
<td>Do the proposed measures have any security impacts and, if so, what are they?</td>
<td></td>
</tr>
<tr>
<td>Compliance of policy options with existing EU initiatives</td>
<td>Do the proposed measures comply with other existing EC (or EU) initiatives?</td>
</tr>
<tr>
<td>Do they create synergies?</td>
<td></td>
</tr>
<tr>
<td>Effects of measures on national legislation</td>
<td>Do the proposed measures have any effects on the Member States or national legislation? If so, are they complementary or at variance?</td>
</tr>
<tr>
<td>Do the proposed measures have the support of Member States or are they expected to create any conflicts with initiatives being undertaken by the Member States in addressing the same issues?</td>
<td></td>
</tr>
</tbody>
</table>

10.2 **INDICATORS FOR ASSESSING IMPLEMENTATION OF POLICY OPTIONS**

A wide variety of indicators can be considered for assessing policy options once they have been implemented. Among possible indicators are the following:

- Number of data losses
- Number of people affected
- Number of data breaches and sources of data breaches (employees, hackers, viruses, government inspection, industrial espionage, phishing, etc)
• Number of identity thefts
• Estimated costs of identity thefts
• Number of audits
• Number of complaints
• Number of prosecutions
• Number of convictions and scale of penalties
• Number of stories in key media re privacy & data protection
• Number of users of e-government services
• Number of users of e-commerce
• Surveys of public opinion and, especially, their trust in e-services
• Of the 100 most popular websites, number with privacy policies
• Of the 100 most popular websites, number offering opt-in vs opt-out policies
• Of the 100 most popular websites, number asking consumers if they agree to installation of cookies.

Acquisti, Friedman and Telang show that there exists a negative and statistically significant impact of data breaches on a company’s market value\(^{749}\) – which is what one would expect. Unfortunately, there is no such indicator for privacy breaches that occur in government, but that does not mean there is no indicator at all. A drop in public trust and/or confidence in government is one indicator. For instance, following the several widely reported breaches or losses of personal data in the UK in 2007 and early 2008, there has been a significant drop in public trust. According to a survey of more than 1,000 UK residents, Data Encryption Systems (DES) found that 90 per cent did not trust the government with their personal data.\(^{750}\)

Heretofore, consumers, regulators and businesses have lacked objective tools to compare the incidence of identity theft across financial and other institutions targeted by fraudsters. Without such tools, consumers cannot “vote with their feet” and choose safer institutions, regulators cannot allocate oversight and enforcement resources to high-risk institutions and practices, and businesses themselves cannot assess how well they perform relative to competitors in fighting this crime. While competition is a powerful force for consumer protection, the lack of information about identity theft makes the market less effective in creating a race to the top among institutions to shield consumers from fraud.

All organisations, not just telecoms companies, but also banks, medical bodies, government departments and businesses should publish details of information security breaches. The prospect of having to notify a security breach would help incentivise organisations to implement stronger security standards in order to protect personal information and prevent breaches.

Indicators on breaches would provide a powerful incentive to improve privacy and data protection.


10.3 ASSESSMENT OF RESPONSE MEASURES

In this section, we have used the assessment criteria discussed in section 10.1 to assess most of the response measures identified in Chapter 8, which are among the most important for dealing with challenges to privacy and trust arising from new developments, i.e., those in Chapters 2 – 6, which are summarised in Chapter 7.

Our assessment of response measures does not exactly parallel those in Chapter 8. We have assessed those that the Commission itself can instigate in whole or in part. Thus, we have not assessed industry or individual initiatives which are discussed in sections 10.4.3 and 10.4.5 respectively, nor have we assessed what we have described as testing third-country data protection safeguards.

We have also clustered the technical and legal responses discussed in 8.1 and 8.5. For example, 10.3.2 (Data control tools) assesses the responses referenced in sections 8.1.1, 8.1.2, 8.1.4 and 8.1.5.

In section 10.4, we assess sets of responses to the challenges summarised in Chapter 7.

10.3.1 Transparency tools

Effectiveness

Transparency tools such as supervisory tools (see section 8.1.3) or online subject access tools (section 8.1.6) improve the explicit handling and control of data. Both data subjects and data controllers know better what data are stored and what is done with data.

The effectiveness of such measures could be measured through user surveys, both among data subjects and data controllers. Another measure for the effectiveness of supervisory tools could be statistics collected from DPA audits, citing the number of incidents uncovered. Supervisory tools can both increase the rate of incidents through better auditing by DPAs or lower it through giving controllers better tools for compliance – any statistics would need to make the appropriate connections.

Transparency tools, if widely deployed, can improve the handling of data as well as improve user awareness of data collections. While the general operations and goals of transparency tools are fairly straightforward, the exact functionality of such tools remains to be individually defined.

Stakeholder support

Online subject access tools would be strongly supported by consumer interest groups and data subjects, while some data collectors might shy away from the additional costs of their implementation. Industrial solutions could drastically lower costs, significantly improving data collectors’ acceptance of such measures.

Similar cost savings would help with the adoption of supervisory tools, as well as statistics that showed how well-supervised data collections result in lower data management costs than management without such tools.
Time

Supervisory tools require the existence of supporting privacy-compliant data management structures (see section 8.1.1). While initial industrial products already exist, more comprehensive infrastructures are needed. Due to the complexity of many existing legacy systems, solid system integration could take several years, but early systems could be available within 12-18 months.

Online subject access is a complex problem and might require novel authentication mechanisms in order not to negatively affect data subject privacy (i.e., to disclose additional data in order to prove ownership of the inspected data). However, some of the more straightforward data collections that involve strong identifiers should pose less of a problem in this sense. Also, current activities surrounding certificate-based identity management could offer support.

Opacity

Increased transparency does not directly limit data collection, nor does it anonymise people, things or devices. However, it might help in limiting unnecessary processing and storage.

Transparency

Supervisory tools will limit function creep through documented and auditable processes that ensure data processing is in line with the purpose for which data were collected. They facilitate governmental and third party oversight, as well as self-regulation and self-reporting.

Online subject access tools are a prime building block for providing user control of collected data, thus enabling a basic legal right for data subjects.

Enforcement

Properly installed and maintained supervisory tools can, to some extent, provide means for detecting or proving violations. Certified installation and operation can help ensure the objectivity of such tools, even if installed in the premises of data collectors.

Both the use of supervisory tools and the availability of online subject access methods can be verified through inspections and audits, and consequently enforced, given sufficient staffing and tasking of DPAs or government agencies.

Economic effects (resources and efforts)

Transparency tools, especially during the initial setup phase when standard solutions will need to be developed, could carry a significant price-tag that would need to be covered by data collectors acquiring and installing such tools (or paying their data processors for implementing them). Ultimately, these costs would most likely be passed onto customers/consumers through higher costs for services and products. These effects could be mitigated through monetary incentives, e.g., tax breaks for adopters or fines for data collectors that fail to implement them. SMEs could be helped by funding the development of standards and/or standardised software that can readily be employed. Public authorities and DPAs
should enjoy lower costs of verifying compliance with data protection law through standardised supervisory interfaces and processes.

Requirements or incentives for using supervisory tools or providing online subject access can stimulate innovation in software and process development. The availability of both supervisory and online subject access tools will improve the quality of data inspection and control for consumers.

Requiring online subject access for services rendered outside the EU might be seen as discriminating against third-country service providers.

**Social impacts (other than privacy protection)**

Online subject access requires (or at least is greatly aided by) novel forms of authentication, e.g., identity management tools that support certificate-based identification.

Transparency tools in general will improve public awareness of privacy issues and rights and might help bridge the digital divide if accompanied by information campaigns that encourage use among citizens and businesses alike.

Open subject access tools might negatively affect security of online data if the eligibility of the requestor is not verified sufficiently, i.e., it must be ensured that only the data subject has access to his or her personal data.

**Compliance of policy options with existing EU initiatives**

Transparency tools complement the Data Protection Directive and other related legislation that stipulates data subject rights to the inspection and correction of personal data. They also help business to comply with the requirements of such laws.

**Effects of measures on national legislation**

Mandatory use of transparency tools for supervision of data processing and/or for providing online data access to data subjects would require Member States to introduce new national legislation.

**10.3.2 Data control tools**

This assessment covers privacy-compliant data management (section 8.1.1), development tools and libraries for privacy-compliant data handling (section 8.1.2), infrastructural support for anonymous communication (section 8.1.4) and identity management tools (section 8.1.5) under the overarching concept of *data control*.

**Effectiveness**

Data control tools facilitate user and/or machine control over personal data flows, either at collection or at processing time. Privacy-compliant data management tools and their corresponding development tools ensure that collected data can be processed according to the promises made at collection time. Infrastructural support for anonymous communication and identity management tools support minimal disclosure of personal data at data collection time.
Data management tools are closely linked to supervisory tools and thus each alone solves only part of the puzzle. Identity management tools, together with anonymous communication, can by themselves already significantly curb the amount of unnecessarily collected personal data.

Surveys can be used to assess the effectiveness of such tools: among DPAs and government bodies, to count both violations and complaints; among data collectors, to elicit improved management and cost savings from both new software support and the smaller amount of data collected; and among citizens, to assess acceptance levels of new identity management tools.

Limiting unnecessary data collections and ensuring the proper processing of rightfully collected data will significantly increase citizens’ trust.

While the requirements and functionality of data management tools are fairly straightforward and subject to several years of research, identity management is a fairly new topic and it is not yet clear on how to best support citizens in managing their identity.

**Stakeholder support**

While data controllers might initially resent the increased costs of deploying and maintaining data management software, the overall lower cost of data storage and processing should, in the long run, provide an important incentive. Widespread availability of suitable development tools for such data management systems would require an increased demand for such solutions.

Identity management tools are likely to be adopted by users to manage their online identity. However, their use must be extremely simple and provide an immediate and perceived added value. The numerous stories in the press about data losses might accelerate adoption.

Law enforcement authorities might oppose (further) deployment of anonymous communication as it lowers their ability to trace communications. Data collectors might welcome the lower requirements that come with anonymous data, however, as would data subjects.

The proposed measures empower the user to control and assess data leakage, so are likely to receive significant support from them.

**Time**

Privacy-compliant data management has received significant attention in information systems and database research. Nevertheless, commercial uptake has been difficult, as the cost of integrating this into business systems is considerable. While early products exist, wider support might require up to 12-24 months of development and testing. Widespread adoption might take two to four years.

A range of identity management tools have already been developed (e.g., IDEMIX, PRIME) and are already deployed in consumer products, e.g., Microsoft CardSpace, Liberty Alliance Identity federations, OpenID. A range of anonymous communication tools and infrastructures are also available, e.g., JAP Anon Proxy, eCash, PayMe. However, critical user mass and user
awareness have not yet been achieved. Continued integration into services and operating systems might make identity systems widely used within the next couple of years.

**Opacity**

Providing opacity is the main goal of data management and identity management tools (if combined with anonymous communication and services). Such tools will help curb unnecessary collection and processing of personal data.

**Transparency**

This response measure significantly enhances the participation of users and their control over personal data. Users can better control what data are released through identity management tools and be assured of their proper processing through data management tools. Data management tools support audits and supervision of data processing and thus enable efficient oversight, as well as self-reporting by data collectors.

**Enforcement**

While data collectors can be required to use data management tools for processing, as well as providing online subject access, data subjects might or might not pick up such tools and make use of their right to online access. Data management tools can assist in detecting or even help in proving violations.

**Economic effects (resources and efforts)**

Data management tools might offer cost-neutral deployment, especially if legal requirements for reporting and auditing are introduced which would help such systems pay for themselves rather quickly. Costs for development and deployment will be shouldered initially by software and service companies, then paid for by data collectors and eventually financed by higher costs for products and services, thus by data subjects themselves. Given the centralised nature of many collections, however, such costs might be spread rather thinly.

End users might have to pay a bigger fee for using identity management systems. There might be indirect costs if these are already integrated in operating systems or websites.

Anonymous communication networks will require upfront financing for service providers, unless legal requirements make anonymous communication and services a staple of modern networks. Much of the basic technology for data control tools is in the public domain, though more specialised features, especially in data management, involve intellectual property. In addition, this response measure would most likely stimulate innovation.

The measure would not affect the functioning of the internal market, and might even have a positive impact on competitiveness with third countries, as services from European providers would offer better control and protection of personal data for all users worldwide.

**Social impacts (other than privacy protection)**

This response measure would not involve trade-offs against other social values, would not affect employment, job quality, equal opportunity, health and safety. Identity management
tools could improve public awareness and education. While anonymous communication tools might be used by criminals to evade detection, the measures could equally help combat crime by curbing identity spoofing and theft, thus resulting in a net positive impact on online security.

Well-crafted identity management systems should lower the digital divide between well educated privacy-haves and less educated privacy-have-nots. Novel means for anonymous communications might even improve public health when it comes to self-reporting of infectious diseases.

**Compliance of policy options with existing EU initiatives**

Data control tools complement the Data Protection Directive and other related legislation which stipulate data subject rights to the inspection and correction of personal data. They also help business to comply with the requirements of such laws.

**Effects of measures on national legislation**

Mandatory use of data management tools for supervision of data processing and/or the provision of anonymous communication to data subjects would require Member States to introduce new national legislation.

10.3.3 **Privacy impact assessments**

**Effectiveness**

Privacy impact assessments are an effective and valuable tool for assessing challenges arising from new projects. They may well be instrumental in overcoming the challenges to privacy arising from new projects, even (or especially) those at grand scale such as the multi-billion-pound projects being undertaken in the UK, such as the new ID card scheme, electronic health records and ContactPoint, the scheme for tracking children through their school years and beyond. Among many other things, a privacy impact assessment will determine whether there are less privacy-invasive alternatives to the original conception of projects and services, how best to protect associated databases and avoid function creep. The UK ICO’s privacy impact assessment manual appears to be the best available and works for projects of any size. Also a feature of PIAs is the opportunity to engage all stakeholders and, in so doing, create better transparency in finding better solutions to the perceived problems or challenges. Possible indicators are the increase or growth in the number of PIAs being carried out each year and whether conducting a PIA leads to changes in the implementation of projects as originally conceived. PIAs (using the ICO PIA manual as the benchmark) are clear, understandable and not ambiguous.

**Stakeholder support**

As yet, PIAs are not widely used in the EU. In fact, few countries appear to be using them. Whether they are made mandatory in the EU (as they are in Canada and the United States) or not, they will be supported by most stakeholders, especially if they are carried out as rigorously as contemplated in the ICO guidelines and if they lead to better, more cost-effective, less privacy-invasive solutions. The exceptions might be the largest stakeholders,
notably governments and industry, who originate projects with privacy impacts as PIAs could lead to changes that they might not like.

Service providers based in third countries providing or wishing to provide services to Europeans might also not wish to carry out PIAs.

PIAs will increase stakeholder participation in decision-making by virtue of the fact that their views and information will be sought on the project, its objectives and proposed implementation. In general, it will be more difficult for stakeholders to object to a particular outcome if they have been involved in the process in identifying the most optimum outcome and if their views are seriously taken into account before a decision is made. PIAs will work best at the earliest stages of project planning, i.e., before any decisions have been taken to proceed with a project and how a project should be configured.

**Time**

Initiating a PIA will, in theory, take more time than proceeding without one. However, initiating a PIA at the earliest stages of project planning may lead to savings in time and costs downstream, i.e., if a project proceeds without a PIA, then there may be opposition to the project from many different stakeholders when the implications of the project become known and such opposition may lead to delays in its implementation.

**Opacity**

A PIA and its outcome should avoid unnecessary data collection and processing, minimise the amount of data to be collected, avoid function creep and so on. In general, however, it can be assumed that governments and private sector service providers are generally desirous of collecting as much data as possible, whether they need all of the data or not to carry out the stated purposes of a project. If government or industry has some hidden agenda or hidden objectives in wishing to undertake a project (for example, they envision repurposing the data in one or more ways), then they will be undercutting support from other stakeholders.

**Transparency**

PIAs do enhance transparency in the collection, storage and/or processing of data. As they increase participation by stakeholders, they should foster user controls and respect for user rights. PIAs should lead to better oversight of projects and better reporting by data controllers and processors. They should also lead to auditing of projects and the way in which they are implemented.

Service providers, from government or industry or whoever carries out a project, may see reporting and auditing as additional cost items, however, such costs may be offset greatly by wider stakeholder support for the project or service. In other words, the cost of the PIA measures should be regarded as an investment in ensuring that the project or new service grows much faster than would otherwise be the case.
Enforcement

PIAs can only be enforced if they become legally mandatory. Whether they become mandatory or not, to the extent they are carried out, they will lead to much better transparency which in turn will help in detecting any deviations from the stated purposes and implementation of the project.

Economic effects (resources and efforts)

The costs of undertaking a PIA will be largely borne by the government or company wishing to undertake a project or to provide a new service. However, those other stakeholders wishing to participate in a PIA will incur costs too, e.g., in researching alternatives to proposed implementation schemes and in making representations to the project manager. They may also incur additional costs in monitoring the way in which the project is implemented or service provided after the PIA.

If the Commission views PIAs as an important tool, as it seems to in its draft RFID recommendation wherein it encourages the undertaking of PIAs, it will certainly incur costs if it seeks to make PIAs mandatory, i.e., in preparing a Communication on PIAs, drafting legislation or a Recommendation, and monitoring the progress in undertaking PIAs in EU Member States and by industry. PIAs would not affect negatively the functioning of the internal market, nor would they create barriers for suppliers and service providers. They would not affect the competitiveness of EU companies or impact SMEs. Still, PIAs do have cost implications, both in undertaking them and in ensuring that they are carried out properly (especially if they were to become mandatory). PIAs would not affect IPRs, but they could stimulate innovation to the extent that better ways are found to implement projects or services in a less privacy-invasive way.

PIAs would be beneficial to consumers, certainly more so than if they were not carried out.

If PIAs were made mandatory, most likely they would have impacts on services envisaged by third-country service providers, i.e., the EC would wish to see those third-country service providers undertaking PIAs along the lines of those carried out by their European counterparts.

Social impacts (other than privacy protection)

PIAs carried out transparently should not involve trade-offs against other social values. If fact, they should strengthen other social values.

They will lead to improvements in public awareness since they will engender the availability of more information about an envisaged system, service or project. A PIA would probably lead to better security of personal data and therefore make life more difficult for cyber criminals.

PIAs should not have any negative effects on employment, job quality (except to improve it), social inclusion, equal opportunity, public health, etc.

---

Compliance of policy options with existing EU initiatives

PIAs would complement the Data Protection Directive and other related legislation. Indeed, they would help to increase awareness of the exigencies and obligations imposed by that Directive and others.

Effects of measures on national legislation

If PIAs were made mandatory, Member States would need to introduce new legislation to make them so.

10.3.4 Evaluation of privacy aspects of ICT research proposals

Effectiveness

Defining guidelines to evaluate research proposals with regard to their implications for privacy is a relatively simple way for the European Commission to introduce elements of a privacy impact assessment into practice. While project proposers could be obliged to do a first rough assessment even at the proposal stage, it would be central to foresee a PIA work package for publicly funded ICT research and development projects.

For this purpose, it would be necessary to develop an authoritative and commonly agreed catalogue of criteria to be used.

This measure would foster approaches to incorporate “privacy by design” instead of doing ex-post assessments of privacy impacts and correct possible weaknesses only when a system is fully developed or even introduced into the market. While guidelines for evaluating privacy aspects of ICT research proposals would not solve the problem in totality, it would improve the level of privacy protection and make clear that this is regarded as a core quality of each new system development.

In this respect, there is synergy with PIAs in general and technological approaches to include privacy aspects in very early development stages.

Stakeholder support

The process of defining the guidelines is essential for acceptance by all stakeholders. The process should, therefore, involve all groups of stakeholders in order to take their needs and objections into account. This will help to balance their interests as well to guarantee the support of all groups. One goal for the European Commission could be to initiate and moderate such a process that should not be limited to the EU alone, but include international players and important transnational organisations (the guidelines developed by the OECD could be a starting point for this process).

Time

ICT research guidelines are a long-term response measure, because the success of their implementation will only become manifest in the products and services that are developed based on those guidelines.
Opacity

There could be an indirect influence of ICT research guidelines on opacity. Rules set by legislation and guidelines for privacy protecting system development should co-evolve and inspire each other.

Transparency

While ICT research guidelines themselves do not create transparency, they provide an excellent basis for other instruments that are geared towards making the collection, processing and use of personal data transparent for the citizen. All the more if other instruments such as public procurement or regular PIAs executed by the DPAs are using the same criteria for their assessments.

Enforcement

If complying with the guidelines is a prerequisite for getting public R&D support, the government bodies in charge are able to reject funding for those developments that do not adequately take privacy aspects into account. It is, however, necessary that project proposers do not pay only lip service to the guidelines and that compliance with the guidelines does not become a minor criterion for awarding contracts.

More possibilities to enforce the implementation of measures can be created together with other measures as listed below (see compliance).

Economic effects (resources and efforts)

The direct cost of implementing guidelines would be borne by actors in the ICT R&D domain. Apart from the efforts needed to carry out the requested assessment, it could also become necessary to reorganise research according to the guidelines.

The amount of these costs depends on two factors, first, the range of the individual guidelines and, second, the cost of the measures necessary to put the guidelines into practice. These cost will vary in each case.

Binding R&D guidelines can have positive impacts on competitiveness and innovation activities of European companies by stimulating innovations and creating more trust in their products. On the other hand, strict rules for privacy protection may result in competitive disadvantage when customers are unwilling to pay higher prices for more privacy-protecting products (especially when competitors cross-finance their development through the collection and use of personal data). Especially in the case of SMEs, the proposed guidelines should take into consideration their needs and limitations in applying them.

This risk is similar to that found in the field of eco-friendly but more expensive technologies. Here, similar effort by policy-makers would be required to make clear that privacy protection is not a cost factor but can be an asset in supporting competitiveness (especially when combined with other instruments such as public procurement).
Social impacts (other than privacy protection)

The social impact in the case of ICT research guidelines is open, since it depends on their concrete content. As a result, each rule should be assessed carefully with regard to possible negative effects, especially for societal inclusiveness, equal opportunities and education.

Compliance of policy options with existing EU initiatives

The measure complements possible public procurement strategies and complies with other measures such as a self-regulated code of conduct. This can provide synergies in the way that procurement can enforce the implementation of guidelines.

Effects of measures on national legislation

Though there is no direct effect on national legislation, it seems useful to implement and apply similar guidelines at different levels of policy-making, which could require new national legislation and administrative practice.

10.3.5 Public procurement

Effectiveness

Public procurement policies and instructions can be an important strategic tool in increasing the demand for privacy-enhancing products, services and systems. Among other things, administrations can demand that each supplier carry out a privacy impact assessment for any new systems, products or services it tenders to the EC (and national administrations). These assessments should be made on the basis of a transparent and common agreed catalogue of criteria (cf. also the sections on privacy impact assessments and ICT research guidelines in this chapter). Public procurement authorities should carefully assess such privacy impact assessments, perhaps by independent experts as well as their own procurement staff. They can require bidders to show how they address privacy impacts and security and what alternatives they might have considered.

Public procurement policies can address the privacy issue only with the public sector in view. However, with the combined procurement power of the EU and national governments, spill-over effects are possible so that privacy-enhancing technologies and solutions become standard in non-governmental areas as well.

To measure the effectiveness of procurement strategies, a number of quantitative indicators can be defined, such as the share of systems that have passed a privacy impact assessment.

Empirical evidence shows that government bodies are adverse to taking risks in procuring innovative products for several reasons: (1) innovations may fail which may be negative for providing government services, (2) innovative solutions often cause additional switching and learning costs, (3) necessity for co-ordination among government bodies and solution providers may be difficult where there are diverging interests.\textsuperscript{752}

Stakeholder support

Procurement strategies and/or policies designed to be privacy-enhancing and/or protecting would need broad consultation involving all relevant stakeholders (see also the sections in this chapter on PIAs and ICT research guidelines). Otherwise, the procurement policy runs the risk of not meeting the objectives and losing support from other stakeholders.

Moreover, there is a risk of fragmentation throughout Europe when policy-makers at the European, national and even regional or local levels decide to develop their own procurement strategies and to use different criteria for the assessment of privacy impacts. Therefore, co-ordination of policy actions at all levels is necessary.

Time

After the definition of privacy impact assessment criteria, the respective public procurement procedures can be implemented rather quickly. Due to the longer life-cycle of ICT equipment and systems in administrations, however, it may take several years until it is fully effective.

Opacity

Public procurement policies can increase the degree of opacity since some rules are not obligatory in current legislation or are ambiguous (e.g., the rule of data minimisation).

Transparency

An increase in transparency depends on the degree of stakeholder participation in the process of designing procurement strategies.

Other ways of contributing to transparency such as more user control, information and reports on collection, storage and use of data or auditing possibilities have to be discussed and decided by administrations. Depending on this process, procurement policies could become a model for other stakeholders, notably industry, but as long as administrations are reluctant to build privacy-enhancing features into their procurement strategies, all of the positive effects mentioned above may not be achieved.

Enforcement

Since public procurement is controlled by public administrations, enforcement is rather easily achievable when there is willingness on the part of administrations. Moreover, it requires functioning control bodies, such as DPAs. Indirect enforceability through public attention and control (e.g., through civil rights organisations) depends on the degree on transparency that the actual procurement policies allow.

Economic effects (resources and efforts)

In the short term, administrations will have to bear the direct costs of implementing procurement policies, because an increase in requirements such as encryption systems for hardware will increase prices. In the long term, some of the costs will be reallocated to private companies because they have to adjust research and production to fulfil procurement rules, while competition for public contracts will lead to normalisation of prices again.
Privacy-enhancing public procurement policies may have negative effects on competitiveness and innovation in the short term, depending on the ability of companies to react flexibly and efficiently to the measures. Especially SMEs could have difficulties to cover the costs of change. In the long term, the trend towards more secure, data protective systems (hardware and software) can lead to a competitive advantage, especially if such measures were subsequently adopted in other countries.

**Social impacts (other than privacy protection)**

A general assessment of possible social impacts is difficult, because they vary depending on the acceptance of privacy-enhancing procurement policies and their economic impact.

The adoption of such strategies should increase the job quality for employees in the public sector, due to more security and trust.

More privacy-enhancing systems in the public sector may also increase safety and prevent crimes. If citizens feel that governments take their privacy concerns seriously and that privacy is a major criterion for the selection of public sector ICT systems, this will help in increasing citizens’ trust.

**Compliance of policy options with existing EU initiatives**

Procurement policies complement and support ICT research guidelines, if the policies require compliance. In this way, both measures can create synergies for EU policy.

**Effects of measures on national legislation**

Since public contracts (above a certain amount) have to be open to suppliers from all Member States, there will be a strong interdependency between EU and national procurement rules. This calls for a close co-operation and co-ordination between all involved government actors and activities.

**10.3.6 Standards**

In this section, we assess standardisation produced by intergovernmental bodies such as the ISO, ETSI and open working groups (OWG) such as OpenID as a response to privacy and trust challenges. Although there are differences between the intergovernmental organisations such as the ISO and ITU and industry-supported bodies such as OpenID and OASIS, they both confer legitimacy on standards that may have benefits for privacy, data protection and trust. Most of the important standardisation bodies are not related to the European Union. Most are either international private non-profit organisations (such as the European Committee for Standardization), professional organisations (such as the Institute of Electrical and Electronics Engineers) or part of the United Nations (such as the International Telecommunication Union).

**Effectiveness**

Standards can address privacy and trust challenges, at least in part and as a complement to other responses. An indicator of their success is the extent of their adoption and/or
implementation. Due to their character and often because of their importance in markets or as legal conditions, the acceptance of standards is often high. The most problematic aspect of standards is that for especially in fast-changing areas such as ICT, there are often no standards for emerging technologies at all or that competing standards co-exist.

**Stakeholder support**

Standardisation processes, formal or informal, tend to be dominated by industry and administration representatives. Only some OWG are real grassroots movements, which may include civil society organisations, including consumer and civil rights associations. In other cases, the public may be involved by more or less extensive consultations.

Additionally, as some cases such as the development of the XML standard showed, it is possible to influence negation by public awareness and opinion-building. The EU could support consumer and data protection agencies in sending representatives to meetings.

**Time**

Formal standardisation processes by institutions normally take a long time before an agreement is reached and even longer before they are implemented.

Market-driven standards produced by industry groups can be developed more quickly. Because of their relative time differences in developing standards, important standardisation bodies such as the ISO often adopt a prevailing standard developed by industry.

**Opacity**

Standards have a direct impact on opacity, i.e., they can influence data collection, storage and use in a positive as well as in a negative sense. The direction depends on whether and how the standards deal with privacy and trust challenges arising from technologies and applications. They may help to anonymise people, avoid unnecessary data collection, use and storage and limit function creep.

**Transparency**

The transparency of standardisation processes could be improved if civil society organisations, consumer rights associations and data protection authorities are involved. Standardisation processes can help to provide user control, lead to the inclusion of report functions or audits or foresee information systems on collection, storage and use of data.

**Enforcement**

The Commission cannot enforce standards and standardisation directly. However, the EC can strongly influence the outcome of the standardisation process by initiating and moderating it. The European (and national) DPAs should normally be involved in the standardisation process and thus represent government interests.

Other instruments such as PIAs, ICT research guidelines and public procurement can make use of certain standards obligatory and thus support their adoption.
Economic effects (resources and efforts)

The direct costs of standardisation processes are borne by the participating institutions. This means that especially SMEs and civil society organisations are often under-represented. A better involvement of these institutions in important standardisation processes could be supported by the EC and/or national governments.

In general, standards can create innovation as well as market barriers. Apart from the costs to develop them, standards always have economic impacts, negative and positive. This depends mainly on how markets actors adapt to standards, which can require investments in new equipment, education, etc. There is evidence that the positive effects overall outweigh by far the negative economic impacts of technical standards.\textsuperscript{753}

Social impacts (other than privacy protection)

Social impacts depend very much on the specific case for which standards are developed.

Compliance of policy options with existing EU initiatives

The support for standardisation processes can complement other measures such as ICT research guidelines and procurement policy, especially if proper standards become factored into research guidelines and procurement policies. If so, there will be synergies.

Effects of measures on national legislation

Effects on national legislation depend on the specific standard.

10.3.7 Audits and metrics

Effectiveness

Independent auditing of data protection practices in both the public and private sectors is a very important response to the challenges to privacy and trust. Independent audits, especially if they are made public or, at the least, if the public knows that they are being made, will be effective in raising public trust and confidence that there is at least one institution, the data protection authority, which is mindful of undue incursions into their privacy and of the way in which data are used, protected and repurposed.

Audits will also help improve metrics, measures of how many data breaches or losses have occurred, the sources of those breaches or losses, the number of requests for access, the costs of providing access, the time it takes to respond, whether there has been any repurposing of data, how data are secured and protected, whether training of staff is de rigueur, etc.

It would be desirable for the data protection authorities to conduct the audits, and for the DPAs to audit all organisations that collect and process personal data. Realistically, however, this is so time- and resource-intensive that it is unlikely any DPA could manage such an activity. Thus, alternative courses of action might be to make audits selective and random.

and/or to outsource audits to independent third parties, much as organisations do now in having independent accountants prepare their annual accounts.

Audits may not fix the problem, since they take place after an organisation has begun collecting and processing personal data (whereas a privacy impact assessment ideally should occur beforehand). Nevertheless, if organisations know they are to be audited and that random inspections by the DPA could take place at any time, audits are likely to have a powerful impact in improving data protection and use.

**Stakeholder support**

Most stakeholders probably would support audits in view of their importance in ensuring good organisational behaviour with regard to the collection, use and protection of personal data. However, some of those subject to audits probably would be happier if audits did not take place, as it would lower their costs and risks to their reputations.

As audits would be carried out by the DPA or some other independent third party at the behest of the DPA, audits would not in themselves increase stakeholder participation in decision-making. However, the results of audits may well stimulate greater subsequent stakeholder participation in decision-making affecting the collection, use and protection of personal data.

**Time**

Independent audits in themselves need not consume a lot of time. However, developing and implementing legislation or regulation making audits mandatory and allowing for independent, random audits of both private and public organisations may take some time.

**Opacity**

Audits could very well lead to prohibitions against unnecessary data collection and processing in specific cases. Ditto data minimisation. Audits would also be effective in curtailing mission creep and repurposing of data.

Audits as such would not anonymise people, things and devices, but the audits may lead to greater anonymisation where an outcome of a particular audit is a recommendation or order than some data be de-personalised.

**Transparency**

Audits would increase transparency and respect for user rights and, in particular, the availability of information about the collection, storage and/or processing of data by organisations.

Audits are a form of oversight. Combined with metrics (as they surely would be), audits would stimulate self-reporting by data controllers and/or processors. The effectiveness of metrics would be improved when they enable comparisons between (for example) a company in a particular sector with its competitors as well as comparisons between sectors.
Enforcement

Audits can be enforced by legislation and they would provide the means for detecting and proving violations in the collection, use and protection of personal data.

Economic effects (resources and efforts)

The cost of audits could be shared between the DPA and by the organisation audited, or, better, the organisation audited would pay for the cost of the audit (as is the case now with audits performed by independent accountants in the production of company accounts).

The costs and resources and efforts need not be excessive or even substantial (relatively speaking) if they are borne by the organisation audited, i.e., the DPA could act on a cost-recovery basis which would allow for minimal or no impact on the public purse.

Audits would improve the competitiveness of EU companies in the long term, but in the short term, they would have a negative cost impact on the organisation being audited. The negative impact could be even greater if the audit shows that the organisation has been delinquent, negligent or not taking sufficient care with the personal data it collects and processes.

Audits would not affect IPRs. They might stimulate innovation if an organisation seeks to improve its handling of personal data.

The direct impact on consumers would be minimal, but they would stimulate improvements in practice which will be beneficial to the consumer.

Audits might have impacts on third countries, if organisations based in third countries handle European personal data (as they do). Thus, audits could raise the level of privacy protection on a global level.

Social impacts (other than privacy protection)

Audits would not involve any negative trade-offs against other social values. They would have minimal impact on employment. They could improve job quality in the sense that organisations know they must be more rigorous in their handling of personal data. Audits would not have any impact on equal opportunity, but the outcome of particular audits could lead to improvements in public awareness and public education and could be useful in detecting hackers, attackers, cyber criminals and so on. They would not make us less secure. If anything, they might lead to improvements in security.

Compliance of policy options with existing EU initiatives

Audits and metrics would comply with existing EU legislation. Indeed, they would greatly strengthen the impact of EU legislation.

Effects of measures on national legislation

Audits could affect Member States, to the extent that they might need to implement new legislation to make them mandatory.
10.3.8 Media attention, publicity and public opinion

Effectiveness

The EC can stimulate media attention to privacy and trust issues by a wide variety of means and can guage public opinion in a variety of ways too, notably through Eurostat / Eurobarometer surveys.

These measures draw attention to the problems associated with privacy and data protection and indicate citizens’ views. Negative press reaction will influence public opinion. In the US, for example, media attention led to service providers’ cancelling or postponing trials of NebuAd’s behavioural advertising service. Media attention is more likely to undermine trust than to increase it, but may force service providers to increase transparency which may in the longer term contribute to building trust.

The media tend to focus mainly on negative stories (e.g., data losses in the UK, customer and employee surveillance in Germany) and less often on positive news.

Even with a continuous stream of information to the media, it is impossible to control what the media will actually do with the information.

The national and/or regional focus of most media makes it necessary to design very broad campaigns tailored to the needs of different media.

Stakeholder support

The public, if not most stakeholders, are likely to support media attention to privacy and data security issues, but service providers and government don’t, of course, like to be in the glare of unfavourable media attention, nor the media’s influence on public opinion and support for projects or services where privacy and data protection are at risk.

Time

Stories in the press can appear very quickly, but it may take much longer to see changes in public opinion. Negative media reports are remembered longer than positive ones.

Opacity

Media attention, publicity and public opinion have no opacity effects.

Transparency

Media attention will generally improve public debate. The media do provide some information about the collection, storage and processing of data. Media attention can be regarded as a form of oversight. However, only “news-worthy” events will be noticed, so that many privacy-infringing practices may go undetected (unreported). Media attention will most likely force data controllers to respond to adverse publicity.
Enforcement

It is impossible to enforce media attention. However, where the media themselves have been found blameworthy in violating individuals’ privacy, they have been suitably reprimanded and could face penalties.\(^{754}\)

Economic effects (resources and efforts)

The media bear the costs of reportage, but stakeholders, notably policy-makers, regulators and service providers will also bear some costs in manpower aimed at stimulating stories in the press as well as in undertaking surveys.

Stimulating media attention generally will have no affect on the functioning of the internal market. Media attention may lead to better consumer choice.

Media attention could impact the competitiveness of EU companies if that attention leads to new regulatory requirements, but such regulatory requirements would also most likely apply to service providers in third countries who (intend to) provide services in Europe.

Media attention may stimulate innovation to the extent that it highlights a problem which forces regulators or other stakeholders to do something about it.

Media attention is not likely to affect consumer costs directly, but if media attention leads to the imposition of new regulatory requirements, the costs of meeting those requirements will most likely flow through to higher prices for consumers.

It is unlikely that media attention will discriminate against third country suppliers or service providers.

Social impacts (other than privacy protection)

Media attention may highlight trade-offs against other social values, such as security, but are not likely to involve such trade-offs directly.

Media attention does not affect employment directly, but indirectly it may lead to the recruitment of new staff to deal with problems highlighted in the press.

Media attention could lead to greater stakeholder participation, i.e., by forcing industry and/or government to facilitate such participation.

No impacts on job quality, social inclusion, equal treatment. No impacts generally on public health and safety unless the focus of media attention is specifically with related privacy issues (e.g., arising from e-health and electronic health records).

Media attention can build support for authorities’ policies re combating crime, terrorism, etc. However, media attention may also draw attention to abuses (e.g., warrantless wiretapping).

Compliance of policy options with existing EU initiatives

Generally, the EU seeks the widest possible dissemination of information about its policies and programmes. As mentioned above, the media are in most cases only interested in news with national or regional importance.

Measuring EU citizens’ views about privacy should be a permanent topic for Eurostat/Eurobarometer surveys.

Effects of measures on national legislation

Media attention may highlight the disparities between Member States in implementing measures.

10.3.9 Sharing best practices

Effectiveness

Identifying, analysing, sharing and publicising best practices in data protection would address challenges to privacy posed by the ubiquitous Information Society. Perhaps equally useful is identifying bad practices, as Privacy International’s Big Brother awards do. Effectiveness of this response could be measured by surveys to determine whether data controllers and processors made changes to their practices as a result of learning about best practices of others. The effectiveness of the measure would depend on how well the instances of best practice were publicised and brought to the attention of other data controllers. Examples of both good and bad practice would also help raise the awareness of other stakeholders, including the public, about the need for strong data protection measures and would help to build trust on the part of consumers towards e-commerce and e-government – i.e., if some companies or government departments were singled out for praise, it should instil public confidence that they are assiduous in protecting personal data.

Stakeholder support

Identifying and sharing examples of best practice would probably be supported by most stakeholders, although some data controllers might not like attention being paid to examples of best practice in the fear that they might have to do more to protect the data they control. This apprehension could be minimised if the analysis of good practice showed that the costs of protecting personal data well were lower than the costs of doing so poorly.

Time

Identifying, analysing and promoting best practice (which already occurs to some extent as mentioned in section 8.3.2 above) could take say a year, but should be an ongoing activity. A campaign of identifying examples of best practice could be built around an award for the best, but it is probable that best practices are domain or context specific. Hence, for example, an annual report citing say 20 examples of best practice in different domains, involving different technologies, would be more useful to data controllers and processors than a single annual “winner” of a best practice award. As more government departments and industry are building bigger databases, the need for publicising best practice becomes more urgent. Data controllers should be encouraged to put forward their practices if they truly believe their practice would
be useful for others to know about and benefit from. The EC and/or Member States (perhaps via the Article 29 Working Group) should contact data controllers (which number in the hundreds of thousands and probably millions across the whole of the EU) which have been notified to the data protection authorities and encourage them to put forward examples of best practice which could then be analysed by independent third parties on behalf of the EC, the DPAs or the Article 29 Working Party. Identifying, analysing, sharing and promoting best practices should be an annual exercise.

**Opacity**

Identifying, analysing, sharing and promoting instances of best practice would not prohibit unnecessary data collection, but identified cases of best practice could show how data collection could be minimised, function creep avoided and ways of anonymising people, things and devices.

**Transparency**

The measure would enhance the participation of stakeholders. If data controllers are encouraged to put forward examples of their good practices, it would enhance their participation. If the best practices were promoted well, it would encourage other stakeholders to participate, especially if they were to see benefits to them (i.e., greater data protection, improved trust, lower costs, etc.). The measure does provide for oversight in the sense that there would most likely be some group of independent third parties who would judge whether a particular example deserved to be cited as an example of best practice. The measure would not oblige self-reporting by data controllers and/or processors but it could stimulate some “self-reporting”. The measure would not necessarily include auditing in the strict sense, but there would need to be some criteria for determining whether a practice was deemed worthy of being cited as a best practice and some analysis made of the various practices.

**Enforcement**

The provision of best practice examples should be voluntary. Detecting or proving violations is not applicable to this response measure.

**Economic effects (resources and efforts)**

The principal costs would fall to the European Commission and/or national data protection authorities – i.e., in contacting and encouraging data controllers and processors to put forward examples of best practice, in researching examples and, most importantly, in the dissemination (sharing) of those practices. The cost of undertaking this activity need not be excessive. Whenever a new data controller registered with a national data protection authority, the DPA could make that controller aware of the programme of identifying best practices and encourage them to put forward their practice if they deemed it to be noteworthy. There would also be some costs in undertaking the research and analysis of examples of best practice. One could hope that hundreds or even thousands of examples would be put forward as candidates for being cited as examples of best practice, but probably the number of candidates would not be more than a few hundred at most. Still, even analysing 100 examples could take some months. The cost of promoting best practices might be “shared” to some extent. The Commission and DPAs would certainly want to undertake their own promotional
activities, but undoubtedly the data controllers and processors who achieved recognition by their peers would likely “blow their own horn” too.

The measure would not affect the functioning of the internal market, nor would it have any negative impact on competitiveness, nor on IPRs, nor on consumer costs. The measure could and even should stimulate innovation. Examples of European best practice could also help to improve practices beyond our borders.

**Social impacts (other than privacy protection)**

Sharing best practice would not involve trade-offs against other social values, although they could complement and enhance other social values, such as improved security. The measure would have minimal impact on employment, but it could improve job quality in the sense that data controllers and processors become aware of better practices. The measure would not affect social inclusion, equal opportunity, public health. However, better practices could lead to improvements in online safety, for example. It should lead to improvements in public awareness and education, and should help to combat cybercrime and improve overall cybersecurity.

**Compliance of policy options with existing EU initiatives**

Sharing best practice would complement and support existing EU initiatives, including e-health and e-government, and support existing EU legislation such as the Data Protection Directive.

**Effects of measures on national legislation**

Sharing best practice would not have any direct effect on national legislation, but rather would support national implementations of the Data Protection Directive and other relevant EC legislation.

**10.3.10 Public education and awareness-raising**

In the context of privacy and trust, one can regard public education and awareness-raising has serving the same goals, i.e., to ensure that citizens take care of their privacy and personal data and to be cautious in extending trust in the ubiquitous Information Society. While the goals may be the same, the means are somewhat different. Education of the public might be seen by most people as something achieved in schools, although the Commission and others have recognised that learning is lifelong and can be achieved by formal as well as informal means (e.g., home learning, learning-on-the-job, short specialist courses sponsored by industry, associations, local authorities and other stakeholders). Awareness-raising may be a somewhat less formal activity than that undertaken by schools and institutes of higher learning, but is arguably equally important in ensuring that citizens reap the benefits and repel the evils of the ubiquitous Information Society. The following assessment covers both education and awareness-raising as two activities with more or less the same goals.

**Effectiveness**

Raising the public’s awareness of challenges to privacy is an essential task to reduce threats. Public education, starting in primary schools and continuing through secondary and tertiary
education, is part of that task. However, public education and raising public awareness will not in itself solve all of the problems, but it is equally true that all of the problems cannot be solved without efforts being made to improve public education.

As education is a responsibility of the Member States, IT courses dealing with safety online are likely to vary in efficacy. Consequently, sharing of best practices and course content would be useful to improve effectiveness.

The EC could serve as a catalyst in the co-ordination of national educational programmes, even at the primary and secondary levels, with a component on privacy and data protection. Vocational education and training programmes could also cover privacy where they do not already do so.

**Stakeholder support**

Public education and raising awareness about privacy and data protection issues will be supported by all stakeholders.

A consultation, initiated by the Commission and/or Member States, would have value in terms of identifying areas that require special attention in raising public awareness and education. A consultation could also be useful to build support for practical measures in sharing best education and awareness-raising practices as well as in eliciting instances of best practices.

Consultations are typically one-off events, but privacy concerns merit continuous monitoring, hence the Commission could hold periodic consultations (say once a year or so) devoted to privacy issues as well as ongoing consultations like Your Voice in Europe or a privacy blog where citizens could be encouraged to raise privacy issues.

**Time**

Improving public education is a gradual, never-ending process. New initiatives, such as sharing best practices (which already takes place to some extent), could take a year or more to institutionalise. Changing or amending course curricula could also take a year or more. IT courses, in which online safety will be but one element, compete with other subjects such as languages, maths and science for funding.

Improving public education through formal education can be complemented by other governmental initiatives aimed at raising public awareness such as websites that provide guidance to the public on online safety, but these too can take many months to put in place or to upgrade.

**Opacity**

Raising awareness and public education does not have any opacity effects.

**Transparency**

Raising public awareness and education can be designed to enhance stakeholder participation. Some oversight and audit measures can be built into this response in order to ensure that
initiatives aimed at improving public awareness and education are working as effectively as possible.

**Enforcement**

Generally not applicable, however, a change in the citizen’s view of privacy can be measured (for instance, by surveys or tests at the end of vocational training courses).

**Economic effects (resources and efforts)**

The cost of improving public awareness and education will be borne by taxpayers.

Costs include exchanges (for example, in identifying, sharing and analysing best practices) between Ministries of Education and local schools authorities. Sharing best practices, however, could reduce costs so that each local education authority does not need to re-invent the wheel, i.e., to duplicate what others are already doing. Other costs include training for teachers, developing websites and educational materials.

Measures aimed at raising public awareness and improving public education would not negatively affect the internal market or reduce consumer choice or create barriers for suppliers and service providers.

The proposed measures could stimulate innovation, not only in the initiatives to raise public awareness, but indirectly through creating a more aware, better educated public.

If the public is more aware of good practices in privacy-enhancing services, it may force some product suppliers and service providers to take additional steps to improve their products and services, thereby raising overall quality.

Public education and awareness-raising will foster the demand for privacy-enhancing technologies which could be a competitive advantage for (European) enterprises producing such technologies and could guide R&D to focus on PETs.

Better educated citizens will be less affected by cybercrime, thus education and awareness-raising helps to reduce direct losses.

**Social impacts (other than privacy protection)**

Public education and awareness-raising do not involve trade-offs against other social values, but there may be some trade-offs within education budgets. The measures would not affect employment, at least not directly. They should improve job quality (better qualified teachers). The measures could help bridge digital divides, i.e., by ensuring all members of the public, especially students, are informed about online safety. They will also help to improve trust in good, privacy-preserving applications. Education measures could improve stakeholder participation, especially if members of the public are given the opportunity to express their views regarding public education needs. Better educated citizens will demand to participate in stakeholder education, so these two instruments (education and stakeholder participation) will reinforce each other.
The measures would lead to improvements in public awareness and education and, as mentioned above, in combating cybercrime (through a more aware, better informed citizenry). As a result they could improve security practices.

**Compliance of policy options with existing EU initiatives**

The measures complement the Commission’s e-inclusion initiatives and its e-competences policies.755.

**Effects of measures on national legislation**

The proposed measures would not affect national legislation. Even if the Commission were to take initiatives aimed at improving public awareness and, specifically, aimed at improving IT courses and especially with regard to online safety and the privacy implications of emerging technologies, it would simply be supporting the Member States. Since education is not a core EU task, the EC should try to initiate the coverage of privacy in national programmes and to co-ordinate these activities.

**10.3.11 Privacy and trust seals**

**Effectiveness**

Depending on the organisation which grants the privacy or trust seal and on the conditions it imposes, such seals can be an effective measure in assuring stakeholders, including the public, that the service provider can be trusted and the individual’s privacy will be respected. However, so far, privacy and trust seals are not widely used across the Internet and have not achieved significant user recognition. As with most of the other response measures discussed in this report, privacy and trust seals should be regarded as only one tool, among others, to deal with the problem of challenges to privacy and trust.

Governments can initiate and support the development of seals. There could also be a government certification (perhaps not for each seal but for the organisation issuing them). Together with a public procurement practice, this could be very efficient.

As for each instrument of self-regulation, the core question is what role governments want to play – whether they leave everything to the market players, even accepting low standard seals, or whether they intervene when seals don’t reach a certain quality level.

Currently, effectiveness is limited by the multitude of seals and a lack of transparency behind many of them.

**Stakeholder support**

Privacy and trust are likely to be supported by many service providers, particularly as they provide marketing leverage (“We have a seal, we can be trusted, unlike our competitors.”) Over time, one could hope that this competitive advantage diminishes in important as competitors reach the standards of a trust seal.

Time

Privacy and trust seal programmes can be implemented relatively quickly. The EuroPriSe project which has been developing a European privacy seal is a 17-month project. Widespread adoption of its privacy seal would, however, take somewhat longer.

Opacity

In theory, a service provider granted a privacy seal would be indicating its compliance with measures such as avoiding unnecessary data collection and processing, minimising the amount of data collected, avoidance of repurposing data and, where possible, anonymising people, things and devices.

Transparency

Privacy seals enhance the participation of stakeholders in the sense that they can apply to be granted a seal. A condition of being awarded a seal would be respect for user rights and making available information about the service provider’s collection, storage and processing of data. The measure would provide for oversight (i.e., if a company were found to be compromising its commitments on the basis of which it was awarded a seal, the seal could be revoked, which would be damaging to its reputation). The measure would provide for audits.

Enforcement

Privacy seals can be enforced. As mentioned above, if a service provider were not fulfilling its commitments, the seal would be revoked. In the instance of the UK Kitemark®, the BSI carries out regular inspections against the quality standard and can revoke the trust mark if companies, professions or public services are found not to be adhering to it.\textsuperscript{756}

Economic effects (resources and efforts)

The cost of implementing a privacy seal program would be borne by the organisation which awarded the seals (e.g., the Commission or Member State or its data protection authority\textsuperscript{757} or an industry association) as well as the user organisation or service provider, but the costs to the latter would be relatively trivial.

The privacy seal would not affect the functioning of the internal market, but would have an effect on consumer choice in the sense that consumers with an understanding of the significance of the seal would be more likely to interact or take service from a company with the seal compared to one without the seal. In theory, companies with the seal would have a competitive advantage over those without a seal. The measure would not affect IPRs, but it might stimulate innovation so that the company could be awarded a seal. A seal program would have negligible effects on the cost of products or services. The measure need not have any negative impacts on third countries, since they would be entitled to be awarded a seal if they provide service in Europe.

\textsuperscript{756} http://www.bsi-global.com/en/ProductServices/About-Kitemark/Kitemark-for-services/

\textsuperscript{757} In general, we think data protection authorities should have a stronger role as the moderator and controller in self-regulation schemes.
Social impacts (other than privacy protection)

Privacy seals would not involve a trade-off against other social values, would not affect employment, job quality, equal opportunity, health and safety. Seals could help to improve public awareness and education. They could help combat crime, since consumers would be more likely to trust a site with a privacy seal than one without a seal. Privacy and trust seals could be expected to have a (favourable) impact on security, since they would indicate that the service provider takes protection of data seriously.

Compliance of policy options with existing EU initiatives

Privacy seals would be in line with existing EU initiatives, such as the aforementioned EC-supported EuroPriSe project and the development of quality criteria (“webseals”) co-funded by the Commission, under its e-Health Action Plan, to increase transparency among health-related websites.

Effects of measures on national legislation

EU-level privacy seals and trust marks might affect (make redundant) similar initiatives by Member States.

10.3.12 Regulatory suasion

Regulatory suasion can be distinguished from a formal consultation in that in a consultation the Commission or data protection authorities typically make a statement or green paper or a communication about a particular issue and then invite comments from (all) stakeholders before deciding on a policy, whereas with regulatory suasion, the data protection authorities (the regulators) engage in somewhat informal discussion, a two-way exchange, aimed at seeking a resolution to a situation that satisfies all parties concerned or, at least, a resolution they can live with.

Effectiveness

Sometimes, regulatory suasion can be as effective as regulation, just as a headmaster may not need to punish a delinquent student; just giving him or her a good talking to may be just as effective. The UK Information Commissioner’s Office having a “little talk” with Phorm about its targeted advertising systems provides a perfect example of regulatory suasion.758 Ditto the US FTC and Congressional hearings on the same issue of personalised advertising.

A variant of the one-to-one discussion is for the regulator to engage one or more industry players in a mixed stakeholder working group to examine a particular issue in order to come up with some guidelines or solutions that garner broad support. The UK government did this with regard to social network sites and particularly with regard to the use of social networking sites by children under the age of 13. The EC has plans for a similar stakeholder group to examine social network sites. (Such working groups may also feature in a consultation process, but it does not necessarily follow that use of a working group is a formal

758 The EC might, however, take some further action. The Commission is analysing the UK government’s response to its call for information about the Phorm trials with BT and is making its own legal assessment of the trials. Williams, Chris, “BT's secret Phorm trials: UK.gov responds”, The Register, 16 Sept 2008. http://www.theregister.co.uk/2008/09/16/phorm_eu_berr/
consultation. As mentioned above, a consultation typically invites comments from all stakeholders, may use several approaches to gather opinions and information, and lasts much longer. One attraction of regulatory suasion or informal discussion between the principal parties – notably the data protection authority and a company or industry – is that it can take place in a much shorter period of time and may be just as effective as going through a longer, more involved consultation process.)

Such measures can be effective. Which indicators are used to measure their effectiveness depends on the issue, but basic indicators might include (a) does industry do anything as a result to address the issue and (b) does their action solve the problem in whole or in part? In the instance of children using social networks, the websites have taken some actions to attempt to curb their use.  

**Stakeholder support**

Regulatory suasion may be supported by industry as preferable to regulators adopting more stringent regulation and minimising the amount of negative attention from the media and privacy advocacy organisations. This response measure does engage stakeholders in the decision-making process as industry, for example, has the opportunity to put its views to the regulator in a non-confrontational atmosphere.

**Time**

It depends on the issue, but industry response could be relatively quick. In any event, regulatory suasion is virtually always going to take less time than developing and adopting a regulation.

**Opacity**

Regulatory suasion may result in a reduction of unnecessary data collection and processing and so on, if industry sees a risk of more stringent regulation or negative media attention.

**Transparency**

The measure may enhance the participation of stakeholders depending on the approach followed. If the regulator (the data protection authority) only has discussions with a company (for example, however, the data protection authority could have similar discussions with other data controllers in government departments) about which it has concerns, then the increase in stakeholder participation is minimal. Even a working group composed of representatives of several different stakeholder groupings may only minimally increase stakeholder participation compared to a more wide-ranging consultation (such as that undertaken by the Commission with regard to RFID). However, minimal participation by other stakeholders may be one of

---

759 In May 2008, Facebook announced new measures to remove inappropriate content from its website, to show automatic warning messages when young users share personal information with strangers and to strengthen its age verification system. Third-party applications developers will have to adhere to revised Facebook safety and privacy guidelines. Its commitments are similar to those made by MySpace in January 2008 and to the guidelines published in April 2008 by the UK Home Office taskforce on child internet safety, to which Facebook, MySpace, Bebo and other web publishers contributed. Kiss, Jemima, “Facebook reinforces safety measures”, *The Guardian*, 9 May 2008. http://www.guardian.co.uk/media/2008/may/09/facebook.digitalmedia
the chief attractions of this measure, at least, for a company, which may prefer to resolve an issue without drawing more attention to it than necessary.

The measure will usually be subject to some informal oversight by the regulator and perhaps other stakeholders (such as the media or privacy advocacy groups), i.e., to ensure that the company does take steps to resolve the issue. The data protection authority could audit the company in due course if it has concerns that the company has not taken discussions with the regulator seriously or if it has not solved the problem.

**Enforcement**

Regulatory suasion cannot be enforced, but if the regulator sees that suasion has not had the intended effect, it could initiate regulation. Hence, a company or industry will almost always realise that the risk of regulation is real and could lead to formal enforcement actions or sanctions (in those Member States where data protection authorities can impose sanctions).

In its informal discussions with a company or industry, the data protection authority, as the regulator, will almost always say that it wants evidence that the company or industry is taking action to correct a situation. Such actions will need to be apparent to the regulator and hence detectable.

**Economic effects (resources and efforts)**

The cost of this action will principally fall on the company or industry. The regulator (data protection authority) will probably incur some relatively minimal costs, for example, in undertaking some research in order to gain some evidence which it can put before the company or industry, to show that it has a legitimate case against the company or industry and that, based on that evidence, it will be necessary for the company or industry to do something to resolve the situation.

Generally, regulatory suasion would not affect the internal market. It might create some “barriers” for suppliers or service providers in the sense that data protection authorities may want to see resolution of a situation before they authorise the company to provide a particular product or service.

The measure nominally would not affect IPRs, but it might require a company to modify its technology (for example, so that the consumer has the possibility of opt-in as opposed to an opt-out or no choice whatsoever).

Regulatory suasion could lead to some innovation to the extent that a company tries to find an innovative solution to the problem that vexes the regulator.

Regulatory suasion is unlikely to have any significant affect on the cost or quality of a product or service offered to consumers, nor on third countries. It is unlikely the measure would be seen as discriminatory, especially if the regulator applies equal pressure to European organisations as well as companies headquartered outside the EU.

---

760 Data protection authorities are obliged by law to monitor compliance with the law, but here we speak of emerging issues, such as behavioural advertising, which are not adequately addressed by data protection legislation and which may be resolved through regulatory suasion, involving informal discussion between the parties concerned.
Social impacts (other than privacy protection)

Regulatory suasion could involve some trade-offs against other social values, but in a positive way, i.e., the regulator would try to convince the company or industry to take an action that would be regarded as socially beneficial.

The measure is unlikely to affect employment or job quality or social inclusion or equal opportunity. It may have positive impacts on public health and online safety.

It may also lead to improvements in public awareness, but it depends on what the issue is. In the case of personalised advertising or behavioural marketing, the issue has had considerable attention in the media, which consequently has helped to raise public awareness of the ease with which persons can be tracked across the Internet and subjected to personalised advertising.

Again, it depends upon the issue, as to whether it would have any impacts on combating crime, but tighter control over social networking might diminish the ease with which cyber criminals can harvest personal data from social network sites.

Compliance of policy options with existing EU initiatives

Regulatory suasion does comply and would create some synergies with existing EU initiatives, such as the Data Protection Directive and other related legislation.

Effects of measures on national legislation

Regulatory suasion would not have any negative effects on the legislation of Member States. Indeed, some national data protection authorities might initiate regulatory suasion themselves in cases where national legislation does not already oblige them to take determined specific actions, notably following the introduction of formal complaints.

10.3.13 Codes of conduct, guidelines and other privacy exhortations

Effectiveness

Codes of conduct can be effective. It partly depends on the organisation that prepares them and the extent of stakeholder involvement. Credibility is a key issue.

In the instance of the OECD guidelines on the protection of privacy and transborder data flows issued in 1980, the success of the measure remains beyond dispute. Many countries have adopted legislation based on the guidelines and many companies have taken the OECD guidelines onboard in their own corporate policies. An indicator of the success is the number of countries and companies that have adopted the guidelines.

Under Article 27 of the Data Protection Directive, the European Commission and Member States are to encourage trade associations and others to draw up codes of conduct (based on provisions in the Directive, of course). Otherwise, the Commission and DPAs can exhort industry to be privacy-protective as the EC did when it encouraged industry to conduct
privacy impact assessments before embarking on new RFID projects.\textsuperscript{761} The number of PIAs carried out in a year (and by whom) could be another indicator and probably more reliable than the number of codes of conduct sent by industry and other data controllers for the blessing of DPAs or the Article 29 Working Group in the course of a year.

Codes of conduct set forth by industry associations can be successful, as the example given in section 8.4.2 above shows, i.e., when Google applied to join the Network Advertising Initiative which requires that its members provide clear and conspicuous notice of their privacy policy. Despite some initial resistance, Google complied.

Nevertheless, despite these positive examples, the effectiveness of codes of conduct can be questioned since they are normally not backed up by law and their effectiveness depends upon their members implementing a code in good faith. Effectiveness also depends on the oversight by the relevant industry association or whatever body has promulgated the code.

Codes of conduct may induce some consumer confidence, but not as much as legislation which offers greater certainty.

**Stakeholder support**

Codes of conduct and guidelines, whether formulated by government agencies (such as the US FTC) or intergovernmental agencies (such as the OECD) or industry bodies will almost always be preferred by industry to enforceable legislation.

Codes of conduct may be drawn up in consultation with stakeholders, notably industry. If industries, associations or other data controllers and processors so wish, they can, as mentioned above, submit it for the blessing of their DPAs or the Article 29 Working Party, but they are not obliged to do so.

**Time**

It will take less time to draft and promulgate a code of conduct than legislation, but the implementation and adoption of a code of conduct may take much longer. In theory, all relevant stakeholders have to comply with legislation when it is brought into force, whereas industry can take its own sweet time in adopting a code of conduct.

**Opacity**

A code of conduct may “prohibit” certain actions, but without the force of law. Ditto data minimisation, function creep and anonymisation measures.

**Transparency**

A code of conduct may lead to greater transparency (as illustrated by Google’s providing a link to its privacy policy on its home page), but again it is unlikely to have the same beneficial effects on transparency as legislation would. In fact, industry may see a code of conduct as an opportunity to be less transparent than they might otherwise have to be if legislation were introduced.

\textsuperscript{761} http://ec.europa.eu/yourvoice/ipm/forms/dispatch?form=RFIDRec
Nominally, a code of conduct does have or should have some oversight, for example, by an industry association to ensure that its members do what they say they will do.

A code of conduct does not normally or necessarily involve formal audits, but as with oversight, an industry association may undertake some investigation to ensure that its members comply with the code (if they say they will).

The British Standards Institution (BSI) does check that those to whom it has awarded the Kitemark seal of trust and quality continue to adhere to quality standards.

**Enforcement**

Codes of conduct may or may not be enforceable, normally not by law, but by, for example, an industry association, especially if the code of conduct is associated with some other measure, such as a trust mark or privacy seal. If a company displays such a trust mark or privacy seal which indicates its adherence to a code of conduct and then is found wanting, the seal could be revoked or it could face some other opprobrium from its industry peers, since it would bring the code into some disrepute.

Even EU codes of conduct may be ignored or transgressed without any blowback.\(^{762}\)

**Economic effects (resources and efforts)**

Developing a code of conduct should not be onerous from a cost point of view. The principal costs would be borne by the companies who need to take some measures to comply with the code. Here we can distinguish between industry-initiated codes of conduct and those developed by the OECD, for example. One could say that the OECD guidelines have led to significant costs by countries that adopted data protection and other related legislation based on the OECD guidelines.

A code of conduct would not affect the functioning of the internal market, since it would, in theory, apply to all relevant organisations. The same would also apply to third countries, i.e., a code could not be seen as discriminatory. It might, however, disproportionately impact SMEs if they had to take specific actions in order to adhere to the code.

A code might stimulate some innovation by companies in order to comply with it.

While consumers might not attach much credibility to a code of conduct, nevertheless, it could benefit them.

\(^{762}\) As an example, Edward Hasbrouck, “the Practical Nomad”, said in a 26 March 2007 submission to the LIBE Committee of the European Parliament and the Article 29 Working Party that the Code of Conduct for Computerised Reservation Systems (CRSs) requires “(A) consent of the passenger for any transfer of data in PNRs to entities (including government agencies) not involved in the reservation, and (B) notice by each system user (airline, travel agency, tour operator, etc.) of the CRS used. Because all major global CRS’s do business in the E.U. and are subject to the E.U. Code of Conduct, these provisions are the de facto global standard for the protection of PNR’s and other travel data… these rules are widely and flagrantly violated. Compliance is extremely rare, perhaps because there has been no enforcement by the European Commission of these provisions of the Code of Conduct.” www.hasbrouck.org/IDP/IDP-PNR-26MAR2007.pdf

See also http://hasbrouck.org/blog/archives/001225.html
Training staff is a necessary implication of other self-regulation measures such as codes of conduct. As a result, effectiveness of and stakeholder support for training is not influenced that much by the way the code of conduct is developed and implemented. Other factors such as opacity and transparency are more or less predefined by the code of conduct and its content. While introduction of a code of conduct causes almost no direct costs, the necessary training of staff who should be intimately familiar with it and comply with it will cause serious costs for the implementing enterprise. In this way also, all other economic and social impacts of training staff refer to the implemented code of conduct and its conditions. Nevertheless, it is one of the most important measures (perhaps the most important) to complement and enforce the use of self-regulated codes of conduct within a company.

Social impacts (other than privacy protection)

A code of conduct would not, in theory, involve a trade-off against other social values, although some companies might view a code as restricting their freedom of operation, even if the intent of the code was to make them better, more socially responsible corporate citizens.

A code is not likely to have any significant effects on employment. It might improve the quality of some employees’ jobs in the sense that they would have more responsibilities in ensuring their company adhered to the code. A code might have some beneficial impacts on social inclusion, but that would depend on the scope and intent of the code. Much the same observation can be made about other social impacts, e.g., on public health, public awareness, combating crime, security and so on.

Compliance of policy options with existing EU initiatives and effects on national legislation

Codes of conduct dealing with privacy and trust, no matter who initiates them, should in theory complement and create synergies with existing EU legislation and programmes.

10.3.14 Legal responses

Effectiveness

The proposed measures in 7.5 address only part of the challenges to privacy and trust, i.e., those that can be addressed by legal provisions; other response measures as described elsewhere in this report are also needed.

The indicators currently used by the EC to measure implementation of personal data protection legislation are: as indicator of immediate results, the relevant national law adopted pursuant to EC provisions; as indicators of outcomes, the application of rules and provisions contained in the law measured by appropriate enforcement mechanisms and remedies available to ensure respect for the law and assistance to individuals through judicial remedies and intervention of data protection authorities (ex officio or following complaints); as indicators of impact, facilitated movement of personal information within the EU and
harmonised protection of individuals at a high level (both inside the EU and in third countries for personal data transferred from the EU).\textsuperscript{763}

The proposed measures aim at contributing to ensuring privacy and trust through different layers of protection based on (1) personal data, (2) privacy and (3) reinforcing the technological dimension of privacy protection.

They clarify current provisions that can be considered ambiguous and aim at ensuring legal certainty.

**Stakeholder support**

Proposed measures will need to be discussed before adoption with the relevant stakeholders to dissipate all possible concerns.

Some stakeholders have expressed their lack of support for certain measures such as specific legislation for certain domains. Their point of view needs to be carefully taken into account to make sure that any instrument developing the identified response does not impose unfair burdens on certain stakeholders.

**Time**

The responses have been designed already taking into account that the implementation of concrete measures might require a considerable amount of time. This time is necessary for the fulfilment of the requirements of the EC legislative framework, on the one hand, and the national transposition of EC legislation, on the other hand.

**Opacity**

The measures contribute strongly to the protection of the opacity of individuals by addressing the issue through different approaches, including notably a substantiation of the fundamental right to privacy in more concrete legal provisions.

**Transparency**

The measures contribute strongly to the transparency of processing by addressing the issue through different approaches, including notably a refinement of the legal development of the fundamental right to the protection of personal data.

The concrete modalities of the legal responses are dependent on implementation at national level.

**Enforcement**

By their very nature, legal measures are to be enforced. An aim of the response is to encourage such enforcement.

Economic effects (resources and efforts)

Responses do not appear to involve any special costs.

Reinforcing the role of data protection authorities might require in certain Member States an increment of resources dedicated to them. As a parallel phenomenon, more homogenous EU-wide practices regarding penalties might increase the resources of certain authorities.

Most of the measures address directly problems related to current and potential barriers and obstacles to the functioning of the internal market, aiming at solving the problem.

By clarifying issues related to the applicable law, the measures should have an impact on the competitiveness of EU companies, not to be discriminated in front of others.

The proposed measures take into account issues related to the enforcement of intellectual property rights, but do not affect such rights.

Social impacts (other than privacy protection)

The measures are expected to have different beneficial social impacts, notably by effectively contributing to the functioning of a trustworthy ubiquitous Information Society.

Compliance of policy options with existing EU initiatives

The legal responses proposed in section 8.5 comply with the priorities of the EC policy framework in the field, and aim at better substantiating different EU fundamental rights.

Effects of measures on national legislation

Effects on national legislation exist, even if differently depending on the Member States.

10.3.15 Anticipating new technologies and their impacts

Effectiveness

The proposed measures will not fix the problem in whole, but can be a very effective way to predict and forestall negative consequences that new technologies and applications may have on individual privacy.

To measure the effectiveness of the measure, one should assess how many new technologies have been correctly anticipated, their predicted impact on stakeholders’ privacy and trust and actual benefits of having properly anticipated them.

An improved forecasting of technological developments and their potential negative consequences will clearly benefit stakeholder privacy. The visibility of the action will increase stakeholder trust in government, while the advance warning will allow for better crafted responses.

Foreseeing new technologies and analysing their implications is a difficult task, but one worth undertaking nevertheless.
**Stakeholder support**

The proposed measure will help the Commission to better assess upcoming technologies and be aware of the impacts they bring. Industry can benefit from clearer guidelines regarding the use and limits of new technology. Citizens can be better prepared and educated about the use and implications of novel technology.

**Time**

Anticipating new technologies and their impacts should be a continuous measure, perhaps performed in repetitive cycles, rather than a one-time action. The European Commission should constantly undertake or support research to make such predictions and assessments.

**Opacity**

The measure itself does not provide opacity, but successfully applying its results will lead to minimised negative impacts, such as mission creep and privacy threats.

**Transparency**

The measure encourages stakeholders to collaborate in order to predict and forestall harmful consequences. It does not by itself, in particular, provide for user controls or provisions for auditing, but should improve information availability.

**Enforcement**

Sponsoring specific research in the field can help anticipate new technologies and their impacts. The proposed measured do not provide technical means for detecting nor proving violations.

**Economic effects (resources and efforts)**

The main costs involved would be the funding of corresponding research activities at EU and national level. End users will not pay directly for any of these assessments. The measure would not affect the functioning of the internal market.

While the proposed measures would stimulate innovations through research, they might in some cases recommend to limit the adoption and deployment of harmful applications.

**Social impacts (other than privacy protection)**

This response measure would not involve trade-offs against other social values, would not affect employment, equal opportunity, health and safety. Anticipating new technologies and their impacts could improve job quality, public awareness and education.

**Compliance of policy options with existing EU initiatives**

The European Commission has already started many initiatives fostering research in privacy. This measure could be combined with existing programmes.
10.4 ASSESSMENT OF RESPONSES TO CHALLENGES

In this section, we present an analysis of the advantages and disadvantages of the responses to the challenges, which were summarised in Chapter 7. We also present any interactions between the various responses.

10.4.1 Legal definitions

This subsection assesses response measures to the challenges presented by the difficulties of certain legal terminologies such as personal data, data controller and data processor, as discussed in section 8.5.1.

<table>
<thead>
<tr>
<th>Responses</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regulatory</td>
<td>The introduction of a legislative proposal redefining the notion of personal data might contribute to legal certainty. The same applies to the definitions of data controller and data processor.</td>
<td>It is impossible to completely eradicate the possibility of different readings and interpretations based on any legal definition, no matter how detailed it is. Opening discussions on a new definition of personal data might have negative effects on the level of protection currently granted. Any new definition might need to avoid creating unnecessary fragmentation of the legal framework, and ensure compatibility with other definitions in relevant international legal instruments.</td>
</tr>
<tr>
<td>More input</td>
<td>DPAs have already contributed to the refinement of the interpretation of the definition of personal data, through the Article 29 Working Party, providing a useful reference for any eventual future judicial review of the scope of the definition. Their contribution to discussions on the definitions of data processor and controller appears to be on its way.</td>
<td>The opinions adopted by the Article 29 Working Party provide only interpretative guidance.</td>
</tr>
<tr>
<td>Judicial review</td>
<td>Case law can be instrumental in clarifying the scope of legal terms.</td>
<td>Judicial review by national courts can support divergent interpretations of notions.</td>
</tr>
</tbody>
</table>

Interactions

This challenge concerns legal definitions and can therefore only be addressed through a limited number of types of responses. Interpretative guidance by DPAs and judicial review appear to be two especially well-suited responses to deal with the identified challenges related
to legal definitions, even though legislative intervention might need to be considered were they to fail in effectively coping with the challenge.

### 10.4.2 Data collection and use

<table>
<thead>
<tr>
<th>Responses</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regulatory intervention – Database controllers could be obliged to</td>
<td>Data subjects do not know currently who has their data and what they are doing with their data. New regulation could ensure that data subjects know who has their data, which would end uncertainty and increase transparency.</td>
<td>Such a regulation would be difficult to enforce. It might even increase risks as additional data (such as postal and/or e-mail addresses) may be required to implement such a provision. The practical logistics could be overwhelming for all involved – not only in terms of one data controller potentially having to notify millions of consumers, but also each consumer being notified perhaps 700 times in the course of a year. Some exceptions (e.g., involving criminals or terrorists) might be controversial.</td>
</tr>
<tr>
<td>maintain data logs of who accesses what data and when they do so.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Database controllers could be obliged to inform data subjects annually</td>
<td></td>
<td></td>
</tr>
<tr>
<td>that they have some data about them.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Privacy impact assessments – Data controllers could be obliged to</td>
<td>PIAs would help ensure that the purpose(s) of data collection are specified and what the impacts might be. Mergers and acquisitions currently assessed only on competition grounds would also be assessed in terms of privacy impacts. Such a response would improve transparency, could help to minimise encroachments on privacy and identify any repurposing of data.</td>
<td>This measure would require much more effort, with time and cost consequences, on the part of many more data controllers. There would be problems of inconsistency and inadequacy of some assessments.</td>
</tr>
<tr>
<td>carry out a privacy impact assessment for any collection of personal</td>
<td></td>
<td></td>
</tr>
<tr>
<td>data. PIAs could be mandatory for mergers &amp; acquisitions where personal</td>
<td></td>
<td></td>
</tr>
<tr>
<td>data are involved.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Testing third-country safeguards</td>
<td>This measure would help to ensure that third-country safeguards are, in fact, adequate and that EU citizens (for example) have access to their data held by third-country controllers and that administrative and cost barriers were not undue. It would be especially valuable if such tests were initiated by citizens, complemented by research</td>
<td>If promised safeguards were found to be wanting, some conflicts between EU data protection authorities and third-country controllers (government and industry) can be foreseen. For citizens who initiate such tests, there would be costs involved. Research by the Commission and/or data protection authorities would also have cost</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Responses</td>
<td>Advantages</td>
<td>Disadvantages</td>
</tr>
<tr>
<td>-----------</td>
<td>------------</td>
<td>---------------</td>
</tr>
<tr>
<td>contracted by the Commission and/or EU data protection authorities.</td>
<td>implications, although these would not be “show-stoppers”.</td>
<td></td>
</tr>
<tr>
<td>Warnings</td>
<td>Warnings placed on websites and even physical locations (“CCTV cameras are in operation”) would help improve the transparency of data collection – i.e., to make users aware that a website or surveillance cameras may be collecting their personal data and/or image and/or voice recording or biometrics.</td>
<td>Data collection warnings are about as popular for industry as health warnings are for the tobacco industry.</td>
</tr>
<tr>
<td>Data control tools, e.g., “sticky” policies</td>
<td>Data control tools by themselves do not necessarily improve transparency, but form the basis for supervisory tools and transparency tools. Requiring data collectors to use, e.g., sticky policies in all their data collections could make illicit collection and the repurposing of collected data more difficult.</td>
<td>These technologies are not commercially mature. Unless more effort is made to make them user-friendly and better known, their effectiveness is likely to be limited to experts.</td>
</tr>
<tr>
<td>Transparency tools</td>
<td>Transparency tools provide data collectors, auditors and data subjects with information on how collected data are used. The availability of, e.g., supervisory tools can help ensure proper collection and use of data.</td>
<td>No standardised technical solutions exist yet, making it costly to integrate such technology into service operation.</td>
</tr>
<tr>
<td>Guidelines and codes of conduct</td>
<td>Codes of conduct are not the sole solution to transparent data collection and use, but they can help in ensuring that data collection and use practices are more transparent to users. Codes of conduct can be formulated and disseminated relatively easily and quickly compared to legislation.</td>
<td>They are not binding. They can be ignored even by those who say they adhere to them. A proliferation of codes can leave consumers confused.</td>
</tr>
<tr>
<td>Audits</td>
<td>Audits can be very effective in identifying practices that are not transparent, and in forcing service providers to remedy deficiencies.</td>
<td>In view of how many organisations process personal data, audits will be a somewhat “hit-and-miss” effort – i.e., not all service providers can be audited.</td>
</tr>
<tr>
<td>Responses</td>
<td>Advantages</td>
<td>Disadvantages</td>
</tr>
<tr>
<td>-----------</td>
<td>------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Media attention</td>
<td>Media attention can be a powerful instrument in bringing about better transparency.</td>
<td>The media often get the facts wrong or focus on the “wrong” issue.</td>
</tr>
<tr>
<td>Privacy &amp; trust seals</td>
<td>Privacy and trust seals can be a very effective way to convey the message that a particular website, service or product can be trusted.</td>
<td>Trust and privacy seals have not reached critical mass. Their use is limited, both by companies and by users. Several such seals undermine the power of one.</td>
</tr>
<tr>
<td>Training staff</td>
<td>Training staff to be more sensitive to transparency requirements is an effective way of minimising improper data collection and use and a way of ensuring better security of collected data.</td>
<td>There are costs involved in training staff and keeping them informed of best practices.</td>
</tr>
</tbody>
</table>

### Interactions

All of these responses to the challenges posed to privacy and trust can be implemented without one negatively impacting another. To maximise transparency in data collection and use, a combination of measures will be necessary. Only the first measure – regulatory intervention by requiring data controllers to notify data subjects annually – is problematic in the sense that it would be difficult to implement even if stakeholders were willing to do so – and one can assume most data controllers would be opposed.

#### 10.4.3 Raising the awareness of and educating stakeholders

The Commission, data protection authorities and other stakeholders face a challenge in raising the awareness of and educating stakeholders about challenges to privacy and trust. If use of e-government and e-commerce services is to become more widespread than they are now, the Commission, DPAs and other large stakeholders need to increase their investment in awareness-raising and education. Similarly, if we are to curtail the losses caused by cyber criminals and other malfactors, for example, through identify theft and malware, including spybots, phishing, smishing, “spearfishing”\(^{764}\), illicit surveillance and electronic espionage, the public must be better educated. There are various responses to this challenge, among which are those listed below.

<table>
<thead>
<tr>
<th>Responses</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Media attention, publicity and public opinion</td>
<td>The Commission, DPAs, industry and other large stakeholders can encourage the media to carry stories about privacy and trust issues arising from the challenges posed by new developments as described</td>
<td>It is difficult to control what the media may say (if anything at all) about particular privacy and trust challenges. There is a risk of amplification of the “wrong” messages (the intent might be to</td>
</tr>
</tbody>
</table>

---

\(^{764}\) “Spearfishing” is a relatively new bit of jargon which describes an activity arising from hackers getting a copy of a company's e-mail list and then sending out official-looking requests for employee personal information. Mikkelsen, Randall, “FBI sees rise in computer crime”, Reuters, 15 Oct 2008. [http://uk.reuters.com/article/technologyNews/idUKTRE49E8J520081015?sp=true](http://uk.reuters.com/article/technologyNews/idUKTRE49E8J520081015?sp=true)
<table>
<thead>
<tr>
<th>Responses</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>in Chapters 2 – 6. They can also use their own websites to describe these challenges, what they are doing and what the public can do. They can engage in blogging on the most popular blogs and offering comments on media stories (most of the most influential newspapers offer readers the opportunity to comment on stories they carry). Government and industry can also regularly survey public opinion in order to identify particular issues and risks of concern to the public and, in doing so, measure whether public awareness is increasing.</td>
<td>encourage greater public awareness, but a story fed to the media might get reported as a surge in cybercrime which could boomerang with the public believing that politicians and policy-makers are unable to control an upsurge in such crime). The EC and DPAs have better control of their own websites and blogging than they do over the media, but their websites may have a much smaller impact than media attention. Although surveys are useful, questions must be framed carefully, a large sample must be taken and similar surveys should take place periodically (say every year, if not more often) in order to monitor progress or changes in public views.</td>
<td></td>
</tr>
<tr>
<td>Sharing best practices</td>
<td>Sharing best practices is an excellent way to raise the awareness of stakeholders, including government departments and industry who may be thinking about deploying similar new technologies and applications. Promoting best practices could and should stimulate and raise the awareness of the public as well as policy-makers, system designers, service providers and so on (i.e., virtually all major stakeholder groups). Ideally, best practices should be drawn from different domains (see the annex for examples). Sharing best practices may result in cost-savings so that different government departments, service providers, schools and so on across the EU do not have to reinvent the wheel. Sharing best practices could stimulate innovation and economic growth.</td>
<td>Identifying best practices in the deployment of technologies and applications that could otherwise be inimical to our privacy could be a very resource intensive exercise. A credibly large number of practices would need to be sampled and analysed in order to find the “best”, and even then they may be good, but not the best. The key challenges re best practices are to identify, analyse, share and promulgate them in a timely way to a sufficiently wide stakeholder base. Some best practices might be rather too abstruse to the public or simply not relevant to their frame of reference. Some developers may not be willing to share their “best practice” because they have vested intellectual property rights or other proprietary interests. There is always a risk that an enterprising journalist, academic or privacy advocacy expert finds flaws in a particular best practice that undermines its credibility and possibly that of the whole</td>
</tr>
<tr>
<td>Responses</td>
<td>Advantages</td>
<td>Disadvantages</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Public education</td>
<td>Public education via the schools is useful and desirable so that even very young people (aged 12 years and under) are aware of privacy challenges posed by the most popular technologies and websites.</td>
<td>By the time school courses are developed and assembled, the most serious privacy threats and challenges may be different from those that feature in school courses.</td>
</tr>
<tr>
<td>Privacy seals and trust marks</td>
<td>Privacy seals and trust marks can be a very useful way to instil trust in the public towards technologies and, especially, websites. Ratings have worked pretty well for films in the cinema and privacy seals and trust marks could work similarly well. Some privacy seals and trust marks (such as the BSI Kitemark or TRUSTe or VeriSign or the EU’s own CE mark for conformity assessment) have become reasonably well recognised and serve as good pathfinders for new initiatives by the EC (such as its support for the EuroPriSe project).</td>
<td>The public may be confused by a proliferation of privacy seals and trust marks, and may not be aware of what each is intended to signify. Many product developers and service providers may feel their products or services are so popular anyway that they have no need for a third-party endorsement which would come with the privacy seal or trust mark. There may be uncertainty as to how effective such marks really are and how much trust the public is willing to confer upon a product or service displaying such a sign. The public may not be aware of the significance of a mark and the basis upon which it is awarded.</td>
</tr>
<tr>
<td>Privacy impact assessments</td>
<td>One of the many spin-off benefits of PIAs is that they can be useful tools for raising the awareness of stakeholders, including the public. They serve as very good vehicles for consultation and engaging stakeholders. They also induce more user control over new proposals or plans that might otherwise raise serious privacy concerns.</td>
<td>Consultation fatigue can be expected if undertaking privacy impact assessments becomes routinised. The number of stakeholders actually participating in a given privacy impact assessment would likely tail off over time as the number of PIAs grows.</td>
</tr>
<tr>
<td>Training staff</td>
<td>All organisations handling personal data (which means virtually all organisations) should train all staff, especially those who actually handle personal data (but even those who don’t because, for example, they could become victims of social engineering and thereby become intermediaries in getting personal data from those who do handle the data), in taking care of digital data, protecting it, in being careful to whom they might give it.</td>
<td>Training is a labour-intensive and costly exercise. Many organisations don’t do enough, that’s clear, but as with road accidents, they may assume that statistically the risks to them are small and manageable and even if they are victimised, the costs may not be as great as training staff regularly (because it is not a one-off exercise) and introducing new, tougher and probably inconvenient security measures.</td>
</tr>
<tr>
<td>Responses</td>
<td>Advantages</td>
<td>Disadvantages</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>pass it, in access control measures and so on. Over time, training will</td>
<td>raise awareness and should reduce the incidence of cyber thefts and data losses, which will not only benefit the organisations concerned, but the economy and society more generally.</td>
<td>Transparency and acceptance of blame will inevitably bring embarrassment and, for listed companies, a drop in their share price and a loss in business. For governments, continuing data losses will lead to a lack of confidence in the government’s management ability and could be a key factor in electoral defeat.</td>
</tr>
<tr>
<td>Transparency and trust-enhancing responses</td>
<td>Virtually all studies show that transparency is the essential ingredient in rebuilding trust. Whenever an organisation suffers a data loss, due to negligence or intrusion, the loss should be reported without delay to the law enforcement and data protection authorities as well as to the individuals affected. Transparency in such cases will be painful and embarrassing to the affected organisation, but admitting culpability or negligence and promising to do something about it (and inviting external experts to provide advice) and, of course, in following through on remedial measures will limit damage more than cover-ups and stonewalling. Rebuilding trust will take a long time, but the sooner the organisation starts, the sooner it can hope to restore its reputation.</td>
<td></td>
</tr>
<tr>
<td>The development and promotion of transparency tools will help to stimulate public awareness of privacy threats.</td>
<td>Transparency tools may be difficult to understand for the majority of consumers, and be more of a turn-off than a turn-on for barely computer literate users.</td>
<td></td>
</tr>
<tr>
<td>Getting a head start in educating stakeholders is important, so having a good idea of the key technologies to look out for could help alleviate public concern early in the development process.</td>
<td>Due to the difficult nature of such forecasts, one might focus on the “easy” technologies and ignore the more difficult but potentially more relevant issues.</td>
<td></td>
</tr>
</tbody>
</table>

**Interactions**

None of the above measures cancels out the others or interacts negatively with the others. Despite the identified disadvantages, all of these measures are desirable and complementary. Each will help to build synergy with the others.
### 10.4.4 Profiling

<table>
<thead>
<tr>
<th>Responses</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public education and awareness-raising</td>
<td>Citizens need to understand the implications of extensive profiling, so that they can make informed choices. Educational campaigns and media attention could help improve the public’s understanding of the extent and reach of commercial data collection, as well as citizens’ rights to inspection and control of the collected data.</td>
<td>Painting a one-sided (negative) picture of personalised services will antagonise both industry and customers.</td>
</tr>
<tr>
<td>Regulatory intervention</td>
<td>With increasing numbers of personal records being assembled and collected, it is important to ensure that existing laws are properly enforced. Especially the discussion surrounding search data requires clear regulatory guidance and enforcement.</td>
<td>The difficulty of determining whether a particular piece of information is personal data makes it hard to decide on the applicability of laws in many situations. Lack of enforcement abilities might make it ineffective.</td>
</tr>
<tr>
<td>Trusted third parties</td>
<td>Trusted third parties could perform independent auditing of profile collections to ensure the proper handling of the collected data.</td>
<td>The lack of standards makes such audits costly – consumers might not be willing to pay more for a service to cover the cost of an independent audit.</td>
</tr>
<tr>
<td>Data control tools</td>
<td>Technology for controlling data flows can help ensure that profiles are only kept for as long as needed, and are used only for the purpose given. Advanced statistical databases could allow for partial anonymisation of profiles without affecting overall operations.</td>
<td>Unless a large enough market exists, deploying data control software might be too costly.</td>
</tr>
<tr>
<td>Trust marks</td>
<td>Trust marks could help consumers make informed decisions when it comes to signing up for personalised services.</td>
<td>Trust marks have not yet reached critical mass. A diversity of marks and their differing terms of service make it difficult for citizens to choose between them.</td>
</tr>
<tr>
<td>Tokens &amp; digital cash</td>
<td>Certificates and digital (anonymous) cash would lower the chances of unwanted profiling.</td>
<td>While some identity management tools already offer the use of certificates to prove certain personal attributes (e.g., being over 18), the use of digital cash is still in its infancy. Anonymous tokens might also prohibit the use of full, attribute-based personalisation and thus lower</td>
</tr>
</tbody>
</table>
Transparency tools

<table>
<thead>
<tr>
<th>Responses</th>
<th>Advantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transparency tools</td>
<td>Transparency tools such as supervisory tools or online subject access tools provide consumer access to and control over their information. The use of transparency tools also helps data collectors ensure the lawful operation of their systems.</td>
</tr>
<tr>
<td></td>
<td>No standardised technical solutions exist yet, making it costly to integrate such technology into service operation. Lack of consumer demand means that the added cost might not be able to come from increased fees. Online subject access might in turn lower the anonymity of consumers if they have to prove their identity in order to inspect their data.</td>
</tr>
</tbody>
</table>

Audits and more resources for DPAs

<table>
<thead>
<tr>
<th>Responses</th>
<th>Advantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audits and more resources for DPAs</td>
<td>DPAs can properly verify the proper processing of personal data. Increased auditing can also push demand for data control tools.</td>
</tr>
<tr>
<td></td>
<td>Auditing large numbers of data collections might not be feasible without technical improvements in auditing software. Audits will also not affect the lawful processing with consumer consent, even though the collected data significantly affect the user’s privacy.</td>
</tr>
</tbody>
</table>

Interactions

Data control and transparency tools greatly simplify the auditing of large profile collections. However, the basic problem of citizens voluntarily disclosing large parts of their private lives can only be addressed by improved education and awareness-raising. Regulatory interventions and increased DPA resources might hasten the process of tool development (in order to lower costs of audits), but overall costs will still increase and will need to be shouldered by consumers. Trust marks and trusted third parties are beneficial under any circumstances, yet their flourishing will strongly depend on consumer demand or regulatory regime. The use of certificates/tokens and digital cash might lower the overall amount of collected data, but will not affect the conscious choice of personalised services by consumers.

10.4.5 Identity management

<table>
<thead>
<tr>
<th>Responses</th>
<th>Advantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Awareness-raising and education measures</td>
<td>Educational campaigns, media reporting, and special activities could teach people the importance of “managing” one’s identity. Simple steps should be offered that provide a baseline protection, without too greatly affecting one’s busy schedule or short attention span.</td>
</tr>
<tr>
<td></td>
<td>There is a flood of well meant information campaigns already today competing for the attention of citizens, e.g., public health. Awareness campaigns on identity management could be perceived as a nuisance, as well as of minimal importance, when compared to campaigns addressing AIDS, smoking or teen pregnancy.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Responses</th>
<th>Advantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data control tools such as identity management tools</td>
<td>Better and more widely available technical tools for managing one’s identity are of prime importance, as current approaches typically fall short of</td>
</tr>
<tr>
<td></td>
<td>Identity tools might add yet another layer of complexity to an already complex online experience. If poorly executed, the public might be driven away from the use of identity</td>
</tr>
<tr>
<td>Responses</td>
<td>Advantages</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Regulatory intervention</td>
<td>Regulatory intervention has the advantage of forcing data controllers to implement technical measures that aid the use and spread of identity management systems.</td>
</tr>
<tr>
<td>Trusted third parties</td>
<td>Trusted third parties, which might include public authorities, might act as identity providers that hold a user’s complete data and only disclose a subset of facts to the various services a user signs up for.</td>
</tr>
<tr>
<td>Trust marks</td>
<td>With an identity provider ecology in the marketplace, consumers are faced with the decision of choosing a trustworthy service. Trust marks, e.g., by DPAs or public bodies, might help consumers in making the right decision.</td>
</tr>
<tr>
<td>Industry initiatives</td>
<td>Industry could voluntarily push the distribution of identity management mechanisms, thus converging on a common standard that might make it easier for identity providers to offer their services on a variety of websites. A number of such initiatives (e.g., MS CardSpace, OpenID) already exist and there are efforts to improve interoperability between these different formats.</td>
</tr>
<tr>
<td>Standards</td>
<td>Open standards for identity management simplify the interoperability between different websites and various identity providers, thus greatly increasing choice and availability.</td>
</tr>
</tbody>
</table>
Interactions

The most important response is the availability of identity management tools – without progress in technical support, identity management is restricted to ad hoc and manual interventions. Raising awareness and education works independently of any other response measure, though its message depends on the available tools that should be recommended or introduced. Industry initiatives and regulatory intervention might be complementary, i.e., a lack of industry initiatives might prompt regulatory intervention. Standards, trust seals and trusted third parties are core enablers that greatly facilitate the creation of strong and useful identity management systems.

10.4.6 Surveillance

Surveillance prompts two main reactions in people – it makes them feel safe (“If there’s a terrorist on this train, he’ll be spotted.”) and it makes them feel paranoid (“Big Brother is watching me all the time.”).

Some level of surveillance can help to protect society. The issue is not to get rid of the surveillance cameras and other such technologies, but to ensure surveillance is controlled, not abused and serves to protect society, and not to endanger its civil liberties.

Assessing the challenges to privacy and other civil liberties by widespread surveillance is a classic example of the risk-risk phenomenon, i.e., in order to deal with one risk (e.g., terrorism and crime), you might create other risks (e.g., to freedom and democracy). Also, increasing surveillance risks diminishing trust (“If the government does not trust me, why should I trust the government?”). Thus, the issue becomes one of striking the right balance and avoiding the risk-risk phenomenon. For more on balancing, see the last section in this chapter.

<table>
<thead>
<tr>
<th>Responses</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy impact assessments</td>
<td>PIAs, involving open consultations with stakeholders, will be helpful to ensure the privacy impacts of (new) surveillance systems are fully taken into account and to determine whether there are alternative ways to achieve the same objectives.</td>
<td>Some stakeholders, such as law enforcement authorities, may not be too happy about PIAs where issues of crime and terrorism are involved. Good PIAs are not cheap. The issues and alternatives are likely to generate controversy.</td>
</tr>
<tr>
<td>Supervisory and data management tools for inspection and verification</td>
<td>Data collected from smart surveillance systems could be properly processed and stored just as any corporate data, using data control and transparency tools. This would allow for greater oversight of individual surveillance operations and reduce the risk of unlawful use of such information.</td>
<td>Employing such privacy tools adds another layer of complexity to the already difficult task of integrating multiple information sources, leading to cost overruns and (more) delays. Some stakeholders might desire more flexible direct access to collected data, instead of rigid</td>
</tr>
<tr>
<td>Responses</td>
<td>Advantages</td>
<td>Disadvantages</td>
</tr>
<tr>
<td>-------------------</td>
<td>----------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Media attention</td>
<td>The media takes great interest in surveillance and gives it a lot of attention, thereby ensuring the public generally is aware of new proposals.</td>
<td>Media attention can be inflammatory and there is a risk that some worthwhile developments in surveillance may be rejected because they have been mischaracterised by the media.</td>
</tr>
<tr>
<td>Sharing best practices</td>
<td>Since most of us live in a surveillance society (with varying degrees of coverage and intrusiveness), it would be highly desirable for public authorities (and even companies who engage in surveillance of employees) to identify good practices that could be shared with others, with the intention, of course, of showing how surveillance and/or privacy intrusions can be minimised and/or data, images and recordings protected and what specifications if any would apply regarding repurposing.</td>
<td>Public authorities and companies will be reluctant to make known the extent of the surveillance (and for what purposes) they carry out.</td>
</tr>
<tr>
<td>Warnings</td>
<td>Citizens, including employees, students, etc., should be informed by means of warning signs or notices that are easily visible and prominent that they are being surveilled or entering a surveillance zone. Many shops and transportation systems already do this.</td>
<td>Some may object to providing such warnings on the grounds of cost or for security reasons or that it might drive customers away. There probably would be some disputes as to what constitutes adequate visibility of a warning.</td>
</tr>
<tr>
<td>Codes of conduct</td>
<td>Those who conduct surveillance should adhere to a code of conduct, which could be drawn up in consultation with all stakeholders.</td>
<td>Some stakeholders would not like to be bound by a code of conduct. There probably would be differences of opinion about the terms of a code of conduct.</td>
</tr>
<tr>
<td>Training staff</td>
<td>Staff who are involved in conducting surveillance or handling the resulting data, images, recordings, etc., should be trained and re-trained at regular levels with regard to ensuring adequate protection, avoidance of undue intrusiveness, not misusing data, etc. Organisations should include in their annual reports what training they have provided. Training should</td>
<td>Some stakeholders might not like to expend more resources than absolutely necessary in providing training, if they provide any at all. Some might just provide lip service to training (e.g., requiring staff to self-certify that they have read company policies re protection of surveillance data).</td>
</tr>
<tr>
<td>Responses</td>
<td>Advantages</td>
<td>Disadvantages</td>
</tr>
<tr>
<td>-----------</td>
<td>------------</td>
<td>---------------</td>
</tr>
<tr>
<td></td>
<td>be supported at the highest levels of the organisations and there should be adequate attention to investigating best practices in training.</td>
<td></td>
</tr>
<tr>
<td>Audits</td>
<td>Those engaged in surveillance should be subject to independent audits with regard to their surveillance practices.</td>
<td>Stakeholders engaged in surveillance may not like audits in case they are reprimanded or they may object to audits on national security or other grounds.</td>
</tr>
<tr>
<td>Metrics</td>
<td>The extent of surveillance should be regularly measured and reported annually by data protection authorities.</td>
<td>Some research would be necessary to formulate adequate metrics, but this is likely to be relatively negligible. Some engaged in surveillance may not wish to provide the data for metrics.</td>
</tr>
<tr>
<td>Legal safeguards</td>
<td>The fundamental rights to privacy and data protection, as pertinently developed by the legislator and the judiciary, aim at protecting individuals against negative effects of surveillance technologies and practices.</td>
<td>Legal safeguards per se are not enough to guarantee effective protection.</td>
</tr>
</tbody>
</table>

**Interactions**

None of these measures interact negatively with the others. They are all complementary and should be carried out. Privacy impact assessments and sharing best practices will probably help in devising codes of conducts, metrics, audits and staff training programmes.

**10.4.7 Informed consent**

<table>
<thead>
<tr>
<th>Responses</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public education and awareness-raising</td>
<td>Public education and awareness-raising can certainly contribute to guide users and consumers when deciding whether to consent to certain types of data processing.</td>
<td>Aware-raising campaigns cannot guarantee that all users and consumers are effectively informed regarding all decisions to be taken.</td>
</tr>
<tr>
<td>Regulatory intervention</td>
<td>The introduction of new provisions better regulating consent might be useful to solve certain problems, such as unfair obtention of consent, and especially the cases for which consent might not be used as a legitimising tool for processing.</td>
<td>EC level regulation cannot regulate in detail all the possible modalities of consent.</td>
</tr>
</tbody>
</table>

EC level legislative intervention
<table>
<thead>
<tr>
<th>Responses</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>can provide a suitably harmonised approach against obstacles to the internal market eventually generated by different national requirements on the modalities of obtention, withdrawal, or proof of consent.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data control tools</td>
<td>Data control tools can contribute to substantiating the content of informed consent.</td>
<td>Data control tools could be presented as a substitute for informed consent, potentially having a counter-productive impact.</td>
</tr>
<tr>
<td>Trust marks</td>
<td>Trust marks can be especially useful as a reference for users and consumers to take into account when deciding whether they consent to data processing or not.</td>
<td>The general disadvantages of trust marks apply (notably concerning the need to ensure effective implementation).</td>
</tr>
<tr>
<td>Transparency tools</td>
<td>Supervisory tools for inspection and verification can be useful to determine whether the information provided to the user/consumer in order to obtain consent matches the reality of practices.</td>
<td>Those capable of using supervisory tools for inspection and verification might be a minority and, more precisely, the minority that is actually less vulnerable to unfair practices (as they already possess a better understanding of the implications of the processing than the average user/consumer).</td>
</tr>
<tr>
<td>Empowering DPAs</td>
<td>More pro-active monitoring by DPAs could contribute to ensuring that provisions on consent are duly applied.</td>
<td>Non-uniform or similar monitoring practices can lead to disparate situations in different Member States, unless coordinating mechanisms such as the Article 29 Working Party are reinforced.</td>
</tr>
</tbody>
</table>

**Interactions**

There does not seem to be any incompatibility between the responses identified. It is important to note that dealing with this challenge might require giving particular attention to other horizontal challenges, and more particularly the challenge of effectively enforcing legislation.

**10.4.8 Enforcing existing legislation**
<table>
<thead>
<tr>
<th><strong>Responses</strong></th>
<th><strong>Advantages</strong></th>
<th><strong>Disadvantages</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>provisions by the responsible entities. Moreover, as the right to personal data protection provides the data subject a series of specific rights, it is crucial that data subjects are educated on the existence of such rights, so they can use them.</td>
<td>campaigns can have difficulties to meet effectively their targeted audiences.</td>
<td></td>
</tr>
<tr>
<td>Regulatory intervention</td>
<td>Only a regulatory framework duly adapted to address the obstacles perceived as impeding its correct implementation has a chance to be effectively implemented. Developments encouraging better enforcement can also have strong beneficial effects.</td>
<td>Adaptation of the EC level regulatory framework needs to take into account the idiosyncrasies of the system, notably concerning inevitable time requirements and eventual problems that might appear during the transposition of provisions in the different national legal frameworks.</td>
</tr>
<tr>
<td>Data control tools</td>
<td>Privacy-compliant data management and identity management tools can be instrumental in ensuring compliance with relevant legislation. Infrastructural support for anonymous communication can be useful for ensuring compliance with certain provisions of the legal framework.</td>
<td>Privacy-compliant data management and identity management tools could benefit only a minority of users and consumers, unless systematically implemented. Infrastructural support for anonymous communication might not be flexible enough to allow for implementation of specific provisions of the legal framework (notably regarding exceptions to confidentiality of communications).</td>
</tr>
<tr>
<td>Trust marks</td>
<td>Privacy and trust seals can encourage implementation of legislation.</td>
<td>Implementation of relevant provisions needs to be required from all entities to which it applies, not only from those who consider it convenient to implement them.</td>
</tr>
<tr>
<td>Transparency tools</td>
<td>Supervisory tools for inspection and verification can be extremely useful to verify compliance with provisions of the regulatory framework. Online subject access tools can be helpful in ensuring enjoyment of subjective rights of the data subject.</td>
<td>Supervisory tools for inspection and verification might only be helpful for a minority of users. The majority would only benefit from them if the enhanced minority uses them for the general benefit. Online subject access tools can only benefit some data subjects, potentially excluding those affected by the digital divide.</td>
</tr>
<tr>
<td>Empowering DPAs</td>
<td>More pro-active monitoring could benefit increased enforcement of</td>
<td>Monitoring activities by the DPAs are themselves an element of the</td>
</tr>
</tbody>
</table>
Responses | Advantages | Disadvantages
---|---|---
legislation. | current regulatory framework whose effective enforcement is being questioned.

Anticipating new technologies and their impact | Early assessments of upcoming technologies can help shape the legal debate, thus improving the chances that enacted regulations can be practically enforced. | Regulations based on potential developments might end up over-regulating, which might stifle economic and technical development.

**Interactions**

More pro-active monitoring by DPAs can contribute to increased awareness-raising, and in principle increased awareness will lead to an increased number of complaints and consultations, which would encourage better monitoring by DPAs and, eventually, better enforcement. Transparency tools can be useful to contribute to effective monitoring, and the widespread use of data control tools could have as a positive side-effect an increased public awareness of the content of the subjective rights in the hands of data subjects.

**10.4.9 International transfers of personal data**

As indicated in Chapter 5 above and elsewhere, personal data can be transferred outside the EU in numerous ways:

- Europeans may use non-EU-based websites, the use of which constitutes consent to the transfer of their data (whether they realise it or not).
- Their personal data may be transferred within a multinational group with offices in Europe and other countries where that group applies binding corporate rules (in effect, a code of conduct) agreed by European data protection authorities.
- Some European government departments and industries may outsource the processing of personal data to companies based outside Europe, as happened in the instance of the UK Driving Standards Agency which had a contract with Pearson Driving Assessments Ltd., which outsourced work to its Iowa subsidiary, which in turn “mislaid” a computer hard drive with details of 3 million Brits in 2007.
- EU-based organisations with offices in third countries may be forced to supply personal data to law enforcement authorities in those third countries, as occurred in the SWIFT scandal.
- Visitors, their travel agents or the airlines carrying them to the US and other non-European countries may be required to provide personal data, including biometrics, before arrival in and upon departure from a third country.
- Europeans travelling with their laptops, mobile phones, BlackBerries or other electronics may be forced to allow customs officials in the US, Canada and other countries to inspect the contents of their gear.
- Law enforcement authorities and intelligence agencies in Europe may exchange personal data with their counterparts in third countries.
- Whenever a European communicates over a network, the communications may be logged, monitored or intercepted by communications carriers and intelligence agencies (e.g., by the US National Security Agency or the massive ECHELON eavesdropping network).  

---

• Cyber criminals outside the EU (as well as inside the EU, of course) may also be sniffing for and capturing personal data for their nefarious purposes.

These transfers pose many risks to Europeans and their personal data, in part because most third countries do not have as strict data protection regimes as we do. Once data are outside European jurisdiction, it becomes difficult or impossible to control what happens to them, how they are processed, for what purposes, with whom they are shared and so on. In addition, those who do attempt to find out what happens to their data or how accurate the collected data are or whether there are possibilities to correct the data may run up against many barriers, not least of which is the cost and time delays in attempting to get sight of their data and even those attempts may fail because their requests for sight of their data may be refused. Furthermore, there is minimal transparency in international transfers of personal data. It is just as difficult (perhaps even more difficult) to know what government agencies are doing with transfers of your data as it is to find out what companies are doing.

Here are some existing and possible responses to these challenges.

<table>
<thead>
<tr>
<th>Responses</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>International co-operation</td>
<td>The EU already has several legitimate ways for transfers of personal data, e.g., under the Safe Harbour Agreement, BCRs and contractual arrangements. In addition, as mentioned in Chapter 5, a High Level Contact Group comprising European and US officials have examined improved co-operation and recommended, inter alia, a new international agreement which would facilitate transfers subject to a set of conditions.</td>
<td>These mechanisms have been developed by officials with limited consultation and minimal opportunity for participation by all stakeholders. The effectiveness of these regimes has been subjected to limited scrutiny. As illustrated by the EU-US PNR case and the SWIFT affair, the current EU legal framework does not appear to deal effectively with international data transfers and with the processing by third countries of data for law enforcement purposes. For example, the European Parliament and Article 29 Working Party both criticised the agreement between the EU and US re PNR and the lack of consultation.</td>
</tr>
<tr>
<td>Privacy impact assessments, open working groups and consultations</td>
<td>These mechanisms have not yet been applied to international transfers of personal data, but offer considerable potential as a concerted response. One could envisage a privacy impact assessment being carried out at a global level with regard to the transfer of personal data for a particular project, service, system, application or even for law</td>
<td>PIAs have yet to be applied to international transfers of personal data and the views of stakeholders, including the government agencies and companies who have or want the personal data, about such a procedure are unknown. One could imagine they might be reluctant to undergo such scrutiny, especially if the data were deemed to be sensitive (e.g., for investigating</td>
</tr>
<tr>
<td>Responses</td>
<td>Advantages</td>
<td>Disadvantages</td>
</tr>
<tr>
<td>-----------</td>
<td>------------</td>
<td>---------------</td>
</tr>
<tr>
<td>enforcement. The project (or whatever) would be subjected to the analysis undertaken as part of a PIA. The PIA would include consultation with stakeholders in the EU and one or more third countries involved in the project. Open working groups of experts and interested stakeholders could also be involved as part of the PIA, with the task of examining safeguards, data minimisation, purpose limitation and so on. The project sponsor (which could be a government agency or a multinational) would be encouraged to keep an open mind with regard to the possible outcomes of the PIA and, if so, the exercise could lead to effective solutions without necessarily requiring new legislation. Almost certainly, the parties involved in the project would need to agree to independent audits and some independent arbitration in the event of disputes.</td>
<td>criminals or terrorists; second and third pillar activities\textsuperscript{766} are outside the scope of the EU’s Data Protection Directive, as stated in Article 3.2).</td>
<td></td>
</tr>
</tbody>
</table>

Sharing best practices

| Sharing best practices | The privacy community is rather large – there are lots of data protection authorities, experts, academics, privacy advocacy groups, etc., as well as technologists writing about privacy-enhancing technologies. There are also many international conferences and workshops dealing with privacy issues, including the International Conference of Data Protection and Privacy Commissioners and the work done over the years at the OECD. So the information exchange is extensive. Still, there | Gathering, analysing and sharing examples of best practices in international transfers of personal, how the data are protected and secured, and the extent of repurposing would be a time-consuming, but not insurmountable research undertaking. Ditto gathering statistical data on requests for access. |

\textsuperscript{766} EU activities are organised in three fields, known as “pillars”. The first pillar covers agriculture, environment protection, economic and commercial questions, immigration and asylum and the free movement of people. The second pillar covers common, foreign and security affairs. The third pillar covers police and judicial cooperation in criminal matters. How compliance with data protection rules is supervised depends on the pillar. First pillar agencies are supervised by the European Data Protection Supervisor (EDPS). The Europol Joint Supervisory Body supervises Europol, the third pillar law enforcement agency based in The Hague.
<table>
<thead>
<tr>
<th>Responses</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>seems to be a need for sharing best practices in privacy and data protection involving international transfers of personal data, and more statistical data and metrics with regard to requests for access to personal data and the responses they generated.</td>
<td>Media attention continues to be one of the best ways of exposing the challenges and deficiencies in international transfers of data. Media attention seems to be necessary in order to develop an antidote to malfeasance and negligence at the global level, such as the SWIFT scandal, state-sponsored cyber wrong-doing, disabling another country’s cyber networks, industrial espionage, interception and the ECHELON affair some years ago. Media attention can help to discover whether there are abuses and misuses in the international transfers of personal data.</td>
<td>Media attention is usually unwelcome by some major stakeholders such as governments and major corporations when international transfers involve sensitive data. Be that as it may, the public and those concerned about civil liberties should not be fobbed off with excuses and rationales based on second and third pillar issues.</td>
</tr>
<tr>
<td>Testing third-country data protection safeguards</td>
<td>Individual stakeholders as well as the Commission and data protection authorities should “test” third-country data protection safeguards where agreements have been reached that personal data from the EU can be transferred. Verification is necessary to ensure that agreements are meaningful.</td>
<td>Third countries may not appreciate or co-operate with “investigations” by the Commission and DPAs re whether they are holding up their part of agreements.</td>
</tr>
<tr>
<td>Standards</td>
<td>ISO-based standards could help ensure equitable terms and conditions for international data transfers as well as verification.</td>
<td>Developing standards can take a long time, especially when some countries are opposed to standards that would require them to improve and make more transparent the ways in which they protect data transferred from other countries.</td>
</tr>
<tr>
<td>Audits and more resources for DPAs</td>
<td>Data protection authorities should have the power and resources to audit international transfers of personal data by other government departments and agencies as well as by the private sector.</td>
<td>Legislation may be needed to give such powers to the DPAs.</td>
</tr>
<tr>
<td>Codes of conduct</td>
<td>Codes of conduct may be useful as</td>
<td>It may be almost as difficult to</td>
</tr>
<tr>
<td>Responses</td>
<td>Advantages</td>
<td>Disadvantages</td>
</tr>
<tr>
<td>-----------</td>
<td>------------</td>
<td>---------------</td>
</tr>
<tr>
<td></td>
<td>a complement or an alternative to ISO-based standards or as a bridging solution until such time as new standards are brought into force. The International Conference of Data Protection and Information Commissioners and/or the OECD could develop such a code. The code could cover data breach notifications, repurposing of collected data, verification and audit measures, security and access to data, among other elements. In developing such a code, inputs should be invited from all stakeholders.</td>
<td>agree a code of conduct applicable at the international level as standards.</td>
</tr>
<tr>
<td>Transparency and trust-enhancing responses</td>
<td>More transparency re international transfers of personal data and what happens to transferred data would help improve public trust in institutional behaviour.</td>
<td>Major stakeholders engaged in international transfers probably would be opposed to more transparency as it could lead to their having to curtail some current practices.</td>
</tr>
<tr>
<td>Training staff</td>
<td>Training staff would help to ensure transferred data are protected adequately and are not repurposed without adequate authorisation.</td>
<td>Training staff has budgetary and time implications.</td>
</tr>
<tr>
<td>Benchmarking, metrics and additional research</td>
<td>Metrics are needed to help determine the scale of the challenge posed by international transfers of personal data. As mentioned above, it would be useful to know how many Europeans have attempted to get access to their personal data and whether they have been successful in their attempts. Measuring the costs and time it takes to get access would also be useful.</td>
<td>Developing the metrics would presumably be relatively straightforward; however, gathering the data may be somewhat more problematic and time-consuming. This disadvantage could be offset somewhat if metrics featured in international agreements re data transfers.</td>
</tr>
</tbody>
</table>

**Interactions**

Some of the above responses may be obviated by others. For example, bilateral agreements could become unnecessary if international standards were agreed. Similarly, some codes of conduct could be superseded by standards. Some stakeholders might argue that privacy impact assessments would be unnecessary if standards were agreed. However, given the rapid change in technologies and externalities (such as terrorist attacks or new types of cyber attacks and cybercrimes), privacy impact assessments would seem to be necessary whatever
standards are put in place. Individual testing of third-country safeguards may be unnecessary (but should not be prohibited, of course) if DPAs are able to carry out effective audits.

10.4.10 Trust

<table>
<thead>
<tr>
<th>Responses</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overcoming the trust deficit – user control of information, fair allocation of risk, transparency and accountability</td>
<td>Either the user controls his or her information or, if that is not possible (e.g., because the data are collected for taxes or census or social services), then the user has to feel the risk of “delegating” control of his information to governments (or industry) is somewhat minimised by transparency (how the data controller uses the data, safeguards in place) and accountability (if the data are compromised or lost, the data controller is held accountable and penalised). In theory, the data subject should see this approach as fair and equitable and, over time, as long as it is seen to be working, then it should help to build or restore trust in government and e-commerce.</td>
<td>This approach will not work if the user is not convinced by the adequacy of the transparency and accountability measures. In fact, trust will be undermined more if only lip service is paid to transparency and accountability – for the data controller to espouse transparency and accountability without putting them into practice will make a bad situation even worse.</td>
</tr>
<tr>
<td>Regulatory intervention</td>
<td>Regulatory intervention has the advantage of forcing data controllers to implement specified measures according to the regulatory regime. Data subjects can thus feel they are protected by legislation.</td>
<td>The disadvantages of regulatory intervention are numerous. The regulatory regime may be ineffective, (i.e., not backed up by adequate enforcement measures), may not address all relevant issues (especially emerging issues that were not considered at the time the regulations were adopted, may require significant expenditure, may require a lot of time to be put in place.</td>
</tr>
<tr>
<td>Trusted third parties</td>
<td>Users may feel that a service provider can be trusted because it uses a trusted third party who has met certain standards (such as those specified in the e-Signature Directive). E-commerce users may bestow trust on a third party retailer because (for example) that third-party retailer has been endorsed by Amazon, which has</td>
<td>The PKI scheme flowing from the e-Signature Directive has not proved to be a success. Few TTP or certificate authorities have enjoyed commercial success.</td>
</tr>
<tr>
<td>Responses</td>
<td>Advantages</td>
<td>Disadvantages</td>
</tr>
<tr>
<td>---------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>already earned the trust of the user.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Guarantees and insurance</td>
<td>The user may extend trust to the service provider because the service provider has put in place guarantees and insurance which limit potential losses to the user.</td>
<td>The user may not like the regime because he might still suffer some loss (e.g., the first €50), even though that loss is limited.</td>
</tr>
<tr>
<td>Trust marks</td>
<td>Trust marks and privacy seals should foster trust because the user has some assurance that the service provider complies with some standard.</td>
<td>There are a variety of different trust marks and privacy seals, which leaves the user confused. After several years, these schemes have yet to reach a critical mass where a particular trust mark or privacy seal is widely recognised. Many service providers and product suppliers do not participate in such schemes.</td>
</tr>
<tr>
<td>Data control tools such as “sticky” policies</td>
<td>Data control and management tools can form the basis for supervisory tools, which in turn allow more efficient administration of trust seals or regulatory oversight.</td>
<td>These technologies are not commercially mature.</td>
</tr>
<tr>
<td>Tokens &amp; digital cash</td>
<td>Using tokens or digital cash minimises the need for users to reveal “private” information (e.g., credit card details).</td>
<td>These schemes are not widely used.</td>
</tr>
<tr>
<td>Transparency tools</td>
<td>Online subject access tools can offer data subjects the means to learn about their collected data and their uses, thus fostering trust in the data collector.</td>
<td>Transparency tools might be difficult to use and only foster the digital divide between those who can operate such tools and less computer literate data subjects.</td>
</tr>
<tr>
<td>Anticipating new technologies and their impact</td>
<td>Early assessments help in educating consumers, thus improving understanding of the technologies and lowering suspicion and distrust.</td>
<td>Educating about too many “potential” issues might overwhelm citizens and lead to an increased detachment from technological developments.</td>
</tr>
<tr>
<td>Cybersecurity bill of rights</td>
<td>A cybersecurity bill of rights, such as that formulated by US Committee on Improving Cybersecurity Research, may inspire trust in e-government and e-commerce, especially because the cyber rights are focused on the user. For industry and government, saying that they adhere to the principles, may be useful as a marketing tool.</td>
<td>The user may feel these cyber rights are more of a “wish list” than anything else, i.e., they are not backed up by law. To be really meaningful, such a cybersecurity bill of rights should be globally accepted. If each country or region were to promulgate a cyber bill of rights that varied in some ways, the user would be left somewhat confused.</td>
</tr>
</tbody>
</table>
Interactions

None of the above responses interacts negatively or positively with any of the others, at least not in theory – in other words, all of these responses can be implemented without their negatively impacting each other. Regulatory intervention can enforce transparency and accountability as well as standards to be met by trusted third parties, guarantees and insurance, trust marks, token and digital cash, and a cybersecurity bill of rights. Apart from regulatory intervention itself, all the other measures can also be implemented by self-regulation too, although their effectiveness may not be as great as they might otherwise be backed up by law. On the other hand, Amazon’s endorsement of third-party sellers using its service has worked very well indeed without the need for legislation.

10.4.11 Harms to individual privacy

A person’s privacy can be harmed in many different ways, too numerous to detail all of them here, but it is useful to identify some of the principal harms.

- **Loss of time** – It may take many months or even years for an individual to recover the financial losses and damage to one’s reputation that accrue from identity theft. There is an opportunity cost involved here too, i.e., the time one spends in recovering from identity theft or intrusions upon one’s privacy could be used more productively or for other pursuits.
- **Financial loss** – The individual may incur expenses to recover from identity theft.\(^{767}\)
- **Damage to one’s reputation and dignity** – The individual’s future actions are limited due to a negative public record that is wrongly associated with the individual’s identity.
- **Denial of services** – the individual may be denied credit or shunned by airlines if he has suffered from identity theft or mistaken identity.
- **Stress and psychological damage** – The individual who has suffered from theft of his identity or from unwarranted exposure may certainly be stressed out and feel much less safe than he felt before becoming aware that his privacy has been violated. The stress, worry and psychological damage may disrupt his relations with his family, friends, employer and so on. Cyber harassment (e.g., by ex-spouses) and online bullying (e.g., by classmates) are new ways of causing psychological damage.\(^{768}\) The individual may become much more fearful than before he or she was victimised (“They are watching me. They are monitoring everything I do.”). One may experience a sense of powerlessness or a loss of control.
- **A loss of trust and confidence** in social institutions that one might have expected to help in recovering from the harms caused by privacy intrusions or that are themselves responsible for the privacy intrusions or that have not been sufficiently careful in securing and protecting personal data.
- **Chilling effects** – If one feels that all of one’s communications are being monitored, a person will generally be much more circumspect about what one says or writes.

\(^{767}\) Among its various ID theft stories, *The New York Times* reported the losses incurred by one victim who said, ‘‘For the first four months, there’s no doubt in my mind that I dedicated 40 hours a week to this,’ Mr. Fairchild said, reflecting the blunt reality that victims must painstakingly prove – often to disbelieving creditors – that debts are not their own. Meanwhile, because his credit rating had been severely damaged, the interest rates on some of Mr. Fairchild’s legitimate cards began climbing, while the credit limits he had been extended on his cards suddenly began to drop.” Zeller, Tom Jr, “For Victims, Repairing ID Theft Can Be Grueling”, *The New York Times*, 1 Oct 2005. www.nytimes.com/2005/10/01/technology/01theft.html

• Disruption of one’s daily life and routines – The individual may be less inclined to go to places or to do things when he believes he will be tracked, photographed and monitored and maybe even stalked. Service providers and product suppliers in possession of personal data may become a nuisance by bombarding the individual with spam and other intrusive marketing in order to get the person to buy, buy, buy.

• Discrimination – Insurance companies and others in possession of personal data may harm the individual through discriminatory pricing. Existing or prospective employers may discriminate against the individual if they glean certain private information about the person, e.g., his sexual orientation.

Harms to a person’s privacy may have social consequences too. A person’s view of society may change. For example,

• He may no longer feel that social institutions can protect him adequately from those “out to get him”.

• People who learn of privacy violations that others have suffered may also become more fearful (“If it can happen to her, it can happen to me.”) and distrustful of other people and social institutions, including political parties (“This is the tenth time the government has lost my data. No way am I going to vote for these incompetents in the next election.”).

• See the footnote on the following page which refers to the centrality of privacy to a democratic society, from which one could conclude (and agree) that harm to an individual’s privacy harms democratic society.

• If one suffers privacy intrusions by electronic means, one may be apprehensive about using e-government and e-commerce services or, if one has already used e-services, one may desist from continuing to use them.

Apart from the work of law enforcement and data protection authorities to apprehend those who violate the privacy of others or are negligent with their personal data, we have identified and assessed the following responses to the harms suffered by individuals from privacy intrusions.

<table>
<thead>
<tr>
<th>Responses</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Research and privacy impact assessments</td>
<td>There is a lot of anecdotal evidence of the financial harms caused by privacy invasions, through ID thefts or data losses or cyber attacks, but rather less formal, structured and comprehensive research about the non-financial aspects. While research or assessments of the impacts of privacy intrusions won’t solve the problem, such research could help to clarify the scale and consequences of the problem and possibly point to some solutions, which could be useful for victims, but may also point to actions that other stakeholders should be taking. Privacy</td>
<td>Cost of research – which is a tiny fraction of the costs incurred by individuals and society as a whole.</td>
</tr>
<tr>
<td>Responses</td>
<td>Advantages</td>
<td>Disadvantages</td>
</tr>
<tr>
<td>--------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>intrusions are both an individual as well as a social problem, hence, solutions should address both the individual and social aspects.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Metrics</td>
<td>There are many periodic estimates of the average cost per person of ID theft, but few metrics covering other harms suffered by individuals as a result of privacy intrusions. These should be developed.</td>
<td>Cost of developing and applying the appropriate metrics.</td>
</tr>
<tr>
<td>Media attention, publicity and public opinion</td>
<td>Media attention continues to be valuable, especially the reportage on individual cases. While such “evidence” of the harms might be regarded as simply anecdotal, nevertheless it draws attention to the harms and provides some indications of what metrics should capture. Media attention also helps to raise the visibility of the issue so that it gets on political “to do” lists and agendas.</td>
<td>The media like bad news as it sells more newspapers than good news, of course, but some stakeholders, especially policy-makers and corporate opinion leaders, may feel press reports exaggerate the problem and lead to negative social amplification.</td>
</tr>
<tr>
<td>Sharing best practices</td>
<td>Examples of best practice in coping with the harms to individuals caused by privacy intrusions may help other individuals similarly victimised as well as society as a whole.</td>
<td>The cost of researching best practices.</td>
</tr>
<tr>
<td>Public education and awareness-raising</td>
<td>There is already a lot of advice proferred from different sources about what individuals can do, especially if they are victims of fraud and identity theft. There is some but rather less about what individuals can do about the other harms, especially those leading to stress and psychological damage. Advice on dealing with these other harms could be an outcome of the research on best practices and the personal privacy impact assessments mentioned above.</td>
<td>Costs of public education and awareness-raising could be rather more substantial than the costs mentioned above.</td>
</tr>
<tr>
<td>Anticipating new technologies and their</td>
<td>Early knowledge of potential privacy issues can help in the design of secure or less risky alternatives, thus lowering the costs of privacy issues.</td>
<td>It might be very difficult to find solutions for potential issues in potential technological developments, especially if no</td>
</tr>
</tbody>
</table>

769 Waldo et al. refer to the centrality of privacy “to human dignity, candor, and intimacy as well as to a democratic society. Privacy is thus also a means as well as an end, and the committee recognizes considerable instrumental value in privacy – privacy in the service of other important goals. Beyond instrumentality, privacy has important value in demonstrating societal respect for the individual.” See Waldo, James, Herbert S. Lin and Lynette I. Millett, *Engaging Privacy and Information Technology in a Digital Age*, Computer Science and Telecommunications Board, National Academies Press, Washington, DC, 2007, p. 308.
<table>
<thead>
<tr>
<th>Responses</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>impact</td>
<td></td>
<td>concrete applications have yet been proposed.</td>
</tr>
<tr>
<td>Training staff</td>
<td>Governmental and private sector organisations should provide training to</td>
<td>Training staff to be empathetic and helpful to victimised consumers and</td>
</tr>
<tr>
<td></td>
<td>staff not only about protecting personal data, but how to deal with</td>
<td>citizens could be rather costly too, especially in cases where individuals</td>
</tr>
<tr>
<td></td>
<td>consumers and citizens who have been victimised.</td>
<td>suffer harms because the organisation itself has been negligent or delinquent</td>
</tr>
<tr>
<td></td>
<td></td>
<td>in its handling of personal data.</td>
</tr>
</tbody>
</table>

**Interactions**

None of the above responses cancels out others or interacts negatively with the others. All of the responses are complementary. However, further research is required before much additional progress can be made with regard public education and training staff.

**10.4.12 Competing values and interests**

As mentioned in section 7.11 above and elsewhere, privacy is often challenged by competing values and interests. Some experts do not like the notion of a balance, where there might be a perception of a one-to-one trade-off, i.e., a gain for privacy represents a loss to a competing value or interest, such as security. Security guru Bruce Schneier says, “Security and privacy, or security and liberty, are not two sides of a teeter-totter. This association is both simplistic and misleading. Security is always a trade-off, yes, but privacy and liberty are not always the things traded off.” But other experts say “Security is a prominent example of the sort of value that can compete with privacy. Police forces the world over have privacy-invading powers, from surveillance to rights to imprison.” Waldo et al. do see the need for balancing competing values. They put it this way: “An important influence on the process of balancing governmental and societal needs for safety and security and individual privacy is the fact that public safety is – almost by definition – a collective benefit, while government infringements of privacy in the name of public safety tend to affect individuals.”

How can we reconcile these differing views about balances and trade-offs? Simply by recalling that privacy, security, trust and many other values have to be considered in particular contexts. In some contexts, security and privacy are complementary values or interests.

---

770 For example, see Bennett and Raab, who opine that “the concept of ‘balance’ is misleading and rhetorical because the two sides of the equation are literally incommensurable... ‘Balance’ is best seen as a political or bargaining outcome between conflicting objectives, or as a general exhortation not to forget one objective when pursuing the other... It is nonetheless important to consider how such balances, or at least balancing processes, can be evaluated.” Bennett, Colin J., and Charles D. Raab, The Governance of Privacy: Policy Instruments in Global Perspective, MIT Press, Cambridge MA, 2006, pp. 243-244.


Security of data can help protect privacy. In other contexts, security may be invidious to privacy if everyone is under the watchful eyes of surveillance cameras wherever they are.

We are of the view that in today’s society we do have to make trade-offs and balance competing values, but (and this is a big but) the context has to be considered before adopting any rigid ideological positions. We might improve societal security by having surveillance cameras everywhere, by monitoring every telephone call, every e-mail, by having every citizen’s DNA and biometrics in a gigantic database, by monitoring everyone does, but the question to be asked is this: Is this the kind of society we really want? Does society collectively want everyone to be tracked and monitored everywhere all the time? Are we willing to forego all of our privacy (however we define it) for the presumption that we will be safer and more secure? Some people will draw the line at different places. Some surveillance might be okay, justified and sensible, but Total Information Awareness is not acceptable. To achieve a balance that most people can live with at any given time, to assess the trade-offs and the challenges posed to privacy and trust by competing values and interests in particular contexts, we believe the following responses are appropriate.

<table>
<thead>
<tr>
<th>Responses</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy impact assessments, research, consultations, open working groups, transparency</td>
<td>Here we cluster PIAs, research, consultations, open working groups and transparency because all of the latter elements form part of a good PIA. A PIA can be undertaken to consider the trade-offs, to achieve an acceptable balance with regard to any initiative or project that could have impacts on our privacy. As we have said elsewhere in this report, a PIA involving all stakeholders can help bring a wide range of views and opinions and, one hopes, new information that might not have been previously considered in order to arrive at sounder decision-making. By undertaking a PIA, we may find that we do not have to sacrifice privacy for some other cause, that there are measures that can be taken to avoid that sacrifice while still achieving the objective (if, of course, stakeholders agree the</td>
<td>Some of the disadvantages of PIAs mentioned earlier apply here too. PIAs take time to carry out, they have a cost, there is a risk of consultation fatigue, all relevant stakeholders should be involved, it’s important to avoid one or two well-resourced stakeholders from dominating the process.</td>
</tr>
</tbody>
</table>

774 On a per capita basis, the UK is already the most surveilled country in the world, yet government plans to build a giant database holding information about every phone call, e-mail and Internet visit have been condemned even by the official in charge of prosecuting terrorism. In response to the plans, Sir Ken Macdonald, the Director of Public Prosecutions, warned of the dangers posed by a Big Brother security state and told ministers not to “break the back of freedom” by creating powers that could be misused to spy on individual citizens and so threaten Britain’s democracy. Information Commissioner Richard Thomas has also said that creation of the database is a “step too far”. See Verkaik, Robert, “Big Brother database threatens to ‘break the back of freedom’”, The Independent, 21 Oct 2008. http://www.independent.co.uk/news/uk/politics/big-brother-database-threatens-to-break-the-back-of-freedom-967673.html
<table>
<thead>
<tr>
<th>Responses</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>objective is desirable). For example, surveillance may be acceptable under certain conditions, e.g., independent oversight, audits, limited retention periods and so on.</td>
<td></td>
<td>Audits also are time and cost-intensive. Some stakeholders do not wish to be held accountable.</td>
</tr>
<tr>
<td>Audits</td>
<td>Independent audits, the outcomes of which are made public, can help to ensure that the stated objectives remain valid, that data are not repurposed, that systems are as secure as reasonably possible, that privacy is not sacrificed needlessly.</td>
<td></td>
</tr>
<tr>
<td>Media attention and public opinion</td>
<td>Media attention may not be as rigorous as an audit, but its independence serves the same purpose, that stakeholders are held accountable, that people are not victimised, that civil liberties are respected and not violated. Public opinion surveys also are essential, especially so that policymakers can see what concerns the public has and what the public thinks about particular courses of action.</td>
<td>The media face many demands for their attention. They may not be interested in a story which they perceive not to be of interest to their readers or viewers. It is hard to sustain the media’s interest in a particular issue. The media may focus on the “wrong” issues. Public opinion surveys, while good, depend on adequate budgets to carry them out as well as carefully framed questions.</td>
</tr>
<tr>
<td>Metrics</td>
<td>Metrics are useful to detect and measure shifts in public opinion, privacy impacts and outcomes.</td>
<td>Costs in developing and gathering the relevant data – but these are relatively small.</td>
</tr>
<tr>
<td>Sharing best practices</td>
<td>Sharing best practices can help to determine optimum trade-offs and alternatives to trade-offs. Sharing best practices would be a useful input into privacy impact assessments.</td>
<td>Costs in gathering, analysing, sharing and promulgating the best practices.</td>
</tr>
<tr>
<td>Anticipating new technologies and their impacts</td>
<td>An early look at technological developments leaves more time to properly discuss the various values and stakeholders involved in the process, potentially resulting in more balanced technical and regulatory solutions.</td>
<td>Values are strongly tied to particular applications a technology is being used in. It might be difficult to balance stakeholder values in a generic fashion, long before applications for a technology emerge.</td>
</tr>
<tr>
<td>Enforcement of regulatory</td>
<td>Ultimately, the courts must judge whether any interference with</td>
<td>Judicial review can require long periods of time. Moreover, the</td>
</tr>
</tbody>
</table>
### Interactions

None of the above responses cancels out any of the others. They are complementary, and all should be used in responding to the challenges to privacy posed by apparent requirements to balance competing values and interests.

---

775 The margin of appreciation refers to the discretion states are permitted in their observance of the rights of the European Convention on Human Rights, and notably when applying its various exceptions. According to the case law of the European Court of Human Rights, the scope of the “margin” will depend on the nature of the legitimate aim pursued and on the particular nature of the interest involved.
11 CONCLUSIONS AND RECOMMENDATIONS

The attention that the media devotes to privacy and trust is considerable. Hardly a day goes by before the media have zeroed in on some new challenge to privacy and trust, especially data breaches and losses, of course – because they are deemed to be most newsworthy. Furthermore, the challenges to privacy and trust clearly is an issue that preoccupies citizens as numerous surveys continue to show. The lack of trust in government and industry to secure and protect personal data harms e-commerce and e-government, which are growing nevertheless, it is true, but not as fast they might.

This report has identified quite a few threats to privacy and trust arising from new technologies, the socio-economic and administrative developments made possible by those technologies, and lacunae in existing legislation, drawing a rather comprehensive picture of the challenges ahead of us.

This chapter has two main sections, the first of which comprises various key findings from our research. It is followed by our key recommendations to the European Commission.

11.1 FINDINGS OF FACT

The precision of new advertising practices are based in part on new monitoring techniques, known as “deep-packet inspection”, which enables a more in-depth view of what the surfer is up to, of every web page visited, every e-mail sent and every search term entered. Instead of basing their adverts on the content of a web page, advertisers now seek to base their adverts on knowing who is looking at the web page (e.g., dog owners will see adverts for dog food even if they visit a website dealing with personality disorders). One of the key issues raised by behavioural advertising is whether the individual Internet user has to opt out or is given the choice of opting in.

Cloud computing further blurs the boundaries between traditional data storage and processing models. Especially in the end-user domain (in contrast to industrial applications running on SaaS/PaaS infrastructures), this might drive the centralised storage and processing of a large amount of personal information, especially if free use of the “cloud” is conditional upon allowing the cloud operator some sort of access (e.g., in aggregated format, or to insert an advertisement) to this information.

The possibilities of tracking and analysing consumers and their consumption patterns could harm the right of free media use. It could have an impact on how people use media such as IPTV and it increases the possibilities for influencing or manipulating public opinion. Some experts conclude that it is necessary to extend the regulations on the confidentiality of telecommunications to cover our use of media. Many people may not want others to know which media they consume, how often and for how long.

In days gone by, most people could assume that their medical records were a matter between them and their doctors. Such, however, is no longer the case, if indeed it ever was. Many more people can, and do, have access to our electronic health records than most people might think. The UK is in the process of implementing a £12.7 billion information technology scheme which would involve a national database with the electronic health records of all citizens. The project has been described as the biggest non-military IT development in the
world. It is envisaged that tens of thousands of NHS staff with security clearance would have access to millions of patients’ files.

Protecting medical privacy is more difficult today than just a few years ago for many reasons:
- More patient information is collected, both in volume and in types of information.
- More people have access to patient information, including medical caregivers, researchers, and administrators in the health care system and, in many cases, employers and government agencies outside it.
- Patient information is more easily accessible because it is increasingly stored in digital form (and so it can be transmitted more easily than in paper form).
- Patient information is held for very long periods of time, and the longer it remains in existence, the greater the opportunities for abuse.
- More patient information is being collected by types and in volumes that are intended to aid medical practitioners in predicting future medical conditions with greater accuracy.
- Patient information (such as DNA information) is being (or soon will be) collected that has relevance to individuals related to the patient (parents, siblings, current and future offspring), thus raising the potential for significant violations of medical privacy and complicating both the technical and ethical issues involved in managing such information.776

Social networks have been accused of collecting sensitive information about their users and sharing the data without their permission. They have also been accused of not alerting users about how that information is being used. If users want to use a third-party application, they may have to let the application developer access all of their information.

The social tagging phenomenon could affect all consumers who use existing technologies such as social bookmarks as well as emerging ones such as the semantic Web. Although social tagging can be used for different purposes, critics are concerned about possible misuses by someone assigning irrelevant, inaccurate or denigrating tags to something, which is at variance with the need for trustworthy and accurate entries. The anonymity of social tagging challenges the balance between trust and privacy, which is a general problem for many Web 2.0 applications, especially as long as there are no generally binding solutions or regulations dealing with it. One way is to give up the anonymity and introduce systems with several levels of registration and acknowledgment, as Wikipedia has done to deal with the problems it has encountered with the accuracy of articles versus the identification of authors.

Part of the allure of the Internet for advertisers is the potential to use consumer data to deliver different ads to different people, based on their behaviour and presumed interests. The biggest search engines and portals on the Internet – Google, Microsoft, Yahoo and AOL – are all at the forefront of the transformation of the Web, where search engines, social networks and advertising networks are fuelled by the ready availability of personal information.

Google has long told investors that it aims to be a pipeline for all advertising in the future on the Internet and elsewhere. Google’s acquisition of DoubleClick, an Internet company that delivers many of the ads consumers see online and which plants many of the cookies on personal computers, stirred controversy for competitive reasons – each company is the leader

in its business – and because of the sheer volume of personal information it would concentrate in the hands of one company. The combination of Google’s records of consumers’ Internet searches with DoubleClick’s information from cookies prompted complaints that one company would hold extensive data about a large proportion of the world’s Internet users. In December 2007, Google had 62.4 per cent of the worldwide online search market. In Europe, the market share of Google and DoubleClick is close to 90 per cent in parts of the Internet advertising business, according to some estimates.

The relationship between privacy and trust is delicate and ambiguous at best. In one sense, privacy is based on keeping personal data confidential and protected, while trust is based on transparency, i.e., the availability of information. Hence, using such a broad brush characterisation, it might seem that privacy and trust are pivoted against each other. Such, however, is disingenuous, and the relationship is much more nuanced and context-dependent (i.e., who are the stakeholders involved? What is the situation where trust is necessary? What is at stake? etc.). Nevertheless, one can say that as privacy is curtailed, encroached upon, invaded, trust breaks down between citizens and governors, between consumers and enterprise, and society becomes increasingly dysfunctional. This is a key warning from *The Surveillance Society* report prepared for ICO.777 Thus, privacy and trust, in this context, can be seen not as pivoted against each other, but, in fact, intimately entwined. Damage to one damages the other.

11.2 RECOMMENDATIONS

Our analysis shows that one cannot hope for any silver bullets that will solve the challenges to privacy and trust. Responding to the challenges to privacy and trust posed by the ubiquitous Information Society will require a mix of measures, and most of these measures are already being used today in one form or another, to a lesser or greater extent. The issue is not really finding some new instrument that will cure all problems over night, rather the issue is identifying the challenges as they emerge, which requires good horizon-scanning, and then deciding in consultation with stakeholders on the appropriate measures, taking into account the criteria which we have identified in Chapter 10 of this study.

There are no easy recipes for success in countering the challenges to privacy and trust in the ubiquitous Information Society. Even so, the fact that there may not be any does not mean that one should avoid going into the kitchen and cooking something. Hence, we make the following recommendations in the knowledge that still other recommendations could be made and that those made a year or two from now could well be different from these. Indeed, if these are adopted, we trust future recommendations would be different. Rather than making a large number of recommendations, we try to make an easily digestible set of eleven.

The recommendations are primarily addressed to the European Commission. Where they are relevant to other stakeholders (e.g., the data protection authorities of Member States or

777 A recent report from the UK House of Commons Home Affairs Committee has almost the same title and makes almost the same observation as the report to ICO: “Loss of privacy through excessive surveillance erodes trust between the individual and the Government and can change the nature of the relationship between citizen and state. The decision to use surveillance should always involve a publicly-documented process of weighing up the benefits against the risks, including security breaches and the consequences of unnecessary intrusion into individuals’ private lives.” House of Commons Home Affairs Committee, *A Surveillance Society?*, Fifth Report of Session 2007–08, Volume I, HC 58-I, London, 20 May 2008, p. 5.
http://www.publications.parliament.uk/pa/cm/cmhaff.htm
industry), the Commission can play an instrumental role in encouraging those other stakeholders to implement these recommendations.

**Recommendation 1: Develop a common framework for privacy impact assessments and make them mandatory**

A comprehensive methodological framework for privacy impact assessments (PIA) should be developed. The ICO handbook could be the starting point for this activity. The framework should take into account the capabilities and resources of different types of actors resulting in different PIA schemes.

PIAs along the lines of this methodological framework should be mandatory for any significant projects involving personal data. The European Commission and Member States should adopt the necessary provisions to make them mandatory.

Procurement policies and publicly funded research should build in privacy impact assessments in their criteria for awarding contracts. Bidders should show how they address possible privacy impacts and security and what alternatives they might have considered.

Mergers and acquisitions currently assessed only on competition grounds should also be assessed in terms of privacy impacts, which would improve transparency, help to minimise encroachments on privacy and identify any intended repurposing of data.

**Recommendation 2: Require audits of international transfers of personal data**

Agreements on international data transfers should require public and private organisations in third countries to specify how they protect and use personal data gathered from the EU and to which other organisations they might transfer such data and for what purposes. Agreements should include provisions for independent audits of how they treat personal data from the EU. They should also include provisions requiring recipient organisations to specify the charges (if any) they impose in responding to individuals’ requests for access to their data and the timeframes in which they would respond to requests and the opportunities for correcting errors. The European Commission should renegotiate and amend the Safe Harbour and other such agreements to build these in.

**Recommendation 3: Companies and government departments should include in their annual reports a description of their data protection measures and an assessment of privacy risks and responses. They should implement the relevant measures (e.g., audits, training staff).**

As a matter of good governance, companies whose shares are publicly traded and government departments should include in their annual reports what steps they have taken to secure personal data, how the data are used, whether they have transferred it to others and why, and whether they conduct internal audit and training re such data protection measures.

In addition, data collectors and processors should periodically self-audit their data collection and processing practices, including detailed information about data flows, data uses and data users. They should use data management tools throughout the whole data processing cycle. Such tools should offer detailed usage information.
All organisations handling personal data should train all staff, especially those who actually handle personal data, in taking care of personal data, protecting it, in being careful to whom they might pass it, in access control measures and so on. Over time, training will raise awareness and should reduce the incidence of cyber thefts and data losses, which will not only benefit the organisations concerned, but the economy and society more generally. Staff who are involved in conducting surveillance or handling the resulting data, images, recordings, etc., should be trained and re-trained at regular levels with regard to ensuring adequate protection, avoidance of undue intrusiveness, not misusing data, etc. Organisations should include in their annual reports what training they have provided. Training should be supported at the highest levels of the organisations and there should be adequate attention to investigating best practices in training.

**Recommendation 4: Improve legal responses**

Policy-makers in general, and the European legislator in particular, should be fully aware of the fact that legal responses for the assurance of privacy and trust in the ubiquitous Information Society must combine three types of approaches:

1. the protection of personal data,
2. ensuring the effectiveness of the right to privacy and
3. protecting privacy by more deeply taking into account the technological dimension of practices.

These three approaches, even if based on different rationales, are complementary and only by combining them can an appropriate regulatory framework be provided for a trustworthy ubiquitous Information Society. In any event, the required legal responses cannot be reduced to legal developments of the right to personal data protection.

The effectiveness of existing provisions and eventual future legislative proposals would be strengthened if accompanied by a clearer discussion of which values and fundamental rights they aim to serve, thus facilitating the work of those who are called to interpret them, implement them and apply them.

Although the temporality and pace of the development of case law is, by definition, a slow one, the clarifications of the judiciary are always relevant, because they deal with concrete and contextualised issues. Policy-makers and legislators should therefore rely on the work of the judges and, at any rate, learn from the way they deal with privacy and data protection issues.

**Recommendation 5: DPAs should have the authority to conduct audits of public and private sector privacy practices**

Data protection authorities should have the authority and resources to make unannounced inspections and audit any data controller or processor from the private and public sectors.

**Recommendation 6: Develop and use online subject access tools**

Data collectors should, whenever possible, be required to provide (free, or for a small fee) subject access as stipulated in Article 12 of the Directive 95/46/EC through online systems within the next two years (cf. Section 8.1.6). This would stimulate industry activity to design and implement standardised interfaces and online access methods. Instead of getting the
proper technology developed and deployed by means of forcing collectors to provide information and/or access, one could also imagine explicitly paying for research that explores, e.g., standardised online subject access tools. However, the former approach seems to yield more industry-useful results.

**Recommendation 7: Identify, analyse and promote good practices**

As government and industry are building bigger databases, the need for publicising good practices becomes more urgent. The EC and the data protection authorities (perhaps via the Article 29 Working Group) should encourage contact data controllers and processors to put forward examples of their best practices from which a selection could be made in an annual report of good practices produced by the Commission which should be widely publicised. Identified cases of good practice could show how data collection can be minimised, function creep avoided and people, things and devices anonymised. Examples of good practice should come from different domains, including, for example, the educational domain. The basic problem of citizens voluntarily disclosing large parts of their private lives can only be addressed by improved education and awareness-raising. As education is a responsibility of the Member States, IT courses dealing with safety online and the privacy impacts of new technologies are likely to vary in efficacy. Consequently, sharing of good practices and course content would be useful to improve effectiveness and could reduce costs so that each local education authority does not need to re-invent the wheel, i.e., to duplicate what others are already doing.

There is already a lot of advice from different sources about what individuals can do if they are victims of fraud and identity theft. There is some but rather less about what individuals can do about other harms to their privacy, especially those leading to stress and psychological damage. Advice on dealing with these other harms could be included in examples of good practice, which may help other individuals similarly victimised as well as society as a whole.

Clearly, informing the European citizen about new challenges for their personal privacy and the drivers behind them is as important as highlighting what each and every one of us can do to face these challenges. However, awareness raising alone is not enough and must be complemented by other instruments.

**Recommendation 8: Develop a methodology to measure and assess privacy risks and user trust**

Currently there is no agreed methodology on how to measure and assess privacy risk and user trust.

The Commission should initiate additional research for developing such a "privacy risk assessment methodology" including metrics and indicators that could also be used for measuring the implementation of responses to privacy challenges. In recent years, the European Network and Information Security Agency (ENISA) has developed a sophisticated methodological toolbox that could be the starting point to develop similar methods for privacy risk assessment. For metrics and indicators, the examples given in section 10.2 could be a starting point.

As mentioned above, metrics are needed to help determine the scale of the challenges posed by international transfers of personal data. It would be useful to know how many Europeans
have attempted to get access to their personal data and whether they have been successful in their attempts. Measuring the costs and time it takes to get access would be useful.

Also as mentioned above, there are many periodic estimates of the average cost per person of ID theft, but few metrics covering other harms suffered by individuals as a result of privacy intrusions. These should be developed.

**Recommendation 9: Report and publish data breaches, data losses and other privacy infringing incidents**

Whenever an organisation suffers a data breach or loss, due to negligence, intrusion, theft or whatever, the loss should be reported without delay to the law enforcement and data protection authorities as well as to the individuals affected. DPAs should compile statistics re the losses on a sectoral basis and what penalties or remedial actions have been imposed. The structure of these statistics should be compatible with the indicators and metrics used for privacy risk assessment.

**Recommendation 10: Anticipate new technologies and their privacy impacts**

Foreseeing new technologies and analysing their implications is a difficult task, but one the Commission should continue to undertake. Such foresight can be a very effective way to predict and forestall negative consequences that new technologies and applications may have on individual privacy. The visibility of such action will increase stakeholder trust in government, while the advance warning will allow for better crafted responses.

The European Commission (and the Member States) should address proactively privacy issues in a way that involves citizens. The huge media coverage and public reaction to recent incidents such as data losses, trade with personal data on a grand scale, surveillance of employees and journalists, etc., make clear that citizens do not consider privacy as an insignificant topic – which it has never been in fact. The European Commission should initiate and co-ordinate activities that raise the citizens' awareness of the privacy implications of new technologies and advance the general degree of knowledge about possible ways towards a responsible and careful handling of personal information.

**Recommendation 11: Regulators should review transfers of personal data**

Regulators should review practices in the transfers (including the sharing and/or sale) of personal data that occur through the “convergence” of companies (mergers, acquisitions and alliances) to assess whether third parties acquiring such data will protect them adequately and whether the sale of the data involves a repurposing of the data not originally foreseen when the data were collected originally. Individuals should be informed when their data are to be sold to others.